RSA NETWITNESS® SUITE

Guide d'utilisation de gestion des sources d'événements

pour la version 11.0

Informations de contact

RSA Link à l'adresse https://community.rsa.com contient une base de connaissances qui répond aux questions courantes et fournit des solutions aux problèmes connus, de la documentation produit, des discussions communautaires et la gestion de dossiers.

Marques commerciales

Pour obtenir la liste des marques commerciales de RSA, rendez-vous à l'adresse suivante : france.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Contrat de licence

Ce logiciel et la documentation qui l'accompagne sont la propriété d'EMC et considérés comme confidentiels. Délivrés sous licence, ils ne peuvent être utilisés et copiés que conformément aux modalités de ladite licence et moyennant l'inclusion de la note de copyright ci-dessous. Ce logiciel et sa documentation, y compris toute copie éventuelle, ne peuvent pas être remis ou mis de quelque façon que ce soit à la disposition d'un tiers.

Aucun droit ou titre de propriété sur le logiciel ou sa documentation ni aucun droit de propriété intellectuelle ne vous est cédé par la présente. Toute utilisation ou reproduction non autorisée de ce logiciel et de sa documentation peut faire l'objet de poursuites civiles et/ou pénales.

Ce logiciel est modifiable sans préavis et ne doit nullement être interprété comme un engagement de la part d'EMC.

Licences tierces

Ce produit peut inclure des logiciels développés par d'autres entreprises que RSA. Le texte des contrats de licence applicables aux logiciels tiers présents dans ce produit peut être consulté sur la page de la documentation produit du site RSA Link. En faisant usage de ce produit, l'utilisateur convient qu'il est pleinement lié par les conditions des contrats de licence.

Remarque sur les technologies de chiffrement

Ce produit peut intégrer une technologie de chiffrement. Étant donné que de nombreux pays interdisent ou limitent l'utilisation, l'importation ou l'exportation des technologies de chiffrement, il convient de respecter les réglementations en vigueur lors de l'utilisation, de l'importation ou de l'exportation de ce produit.

Distribution

EMC estime que les informations figurant dans ce document sont exactes à la date de publication. Ces informations sont modifiables sans préavis.

février 2018

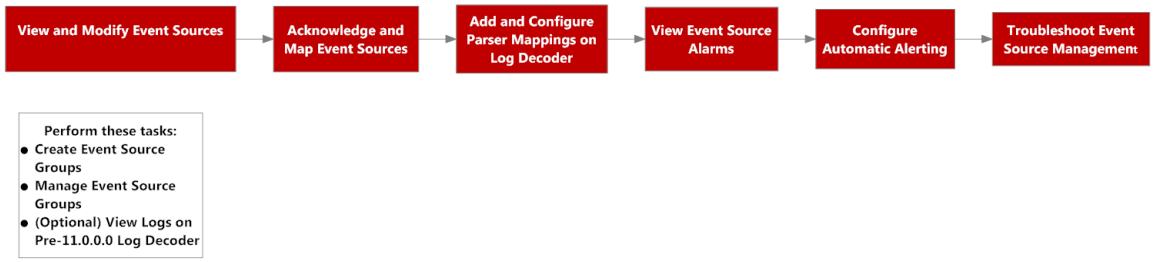
Sommaire

À propos de la gestion de la source d'événements

Le module Source d'événement dans NetWitness Suite permet de gérer facilement les sources d'événement et de configurer des stratégies d'alerte pour vos sources d'événement.

Workflow

Ce workflow montre l'ensemble du processus de configuration des sources d'événements. Il indique également l'emplacement dans le processus de la configuration des paramètres d'alarmes et d'alertes.



Conditions préalables

Deux autorisations s'appliquent au module Gestion de la source d'événements :

- Les utilisateurs utilisent **Afficher les sources d'événement** pour afficher les sources d'un événement, leurs attributs et leurs seuils et politiques.
- **Modifier des sources d'événement** permet aux utilisateurs d'ajouter, de modifier et de mettre à jour les sources d'événement.

Pour plus de détails, reportez-vous aux rubriques suivantes :

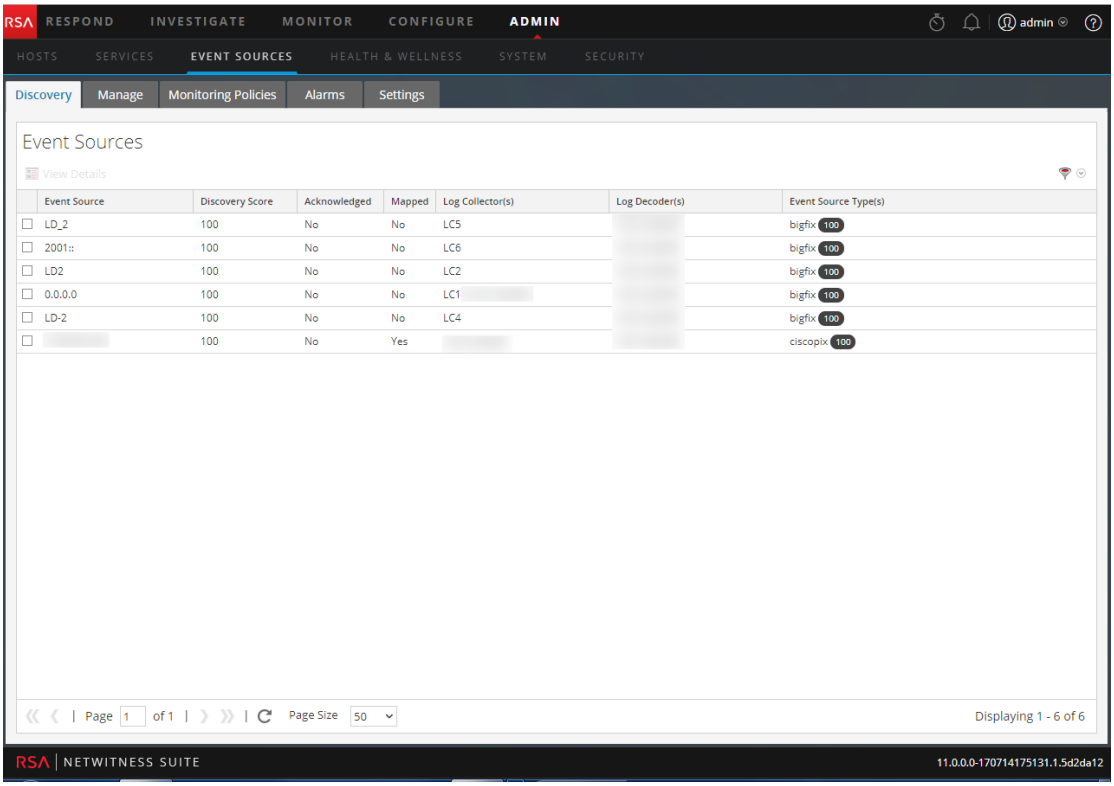
- La rubrique *Onglet Rôles*, disponible dans le **Guide de la sécurité du système et de la gestion des utilisateurs** > **Références** > **Vue Administration - Sécurité** > **Onglet Rôles**.
- La section *Autorisations du rôle* décrit les rôles système de NetWitness Suite intégrés, qui contrôlent l'accès à l'interface utilisateur. Disponible dans le **Guide de la sécurité du système et de la gestion des utilisateurs** > **Mode de fonctionnement du contrôle d'accès basé sur un rôle**.
- La rubrique *Gérer les utilisateurs avec des rôles et des autorisations* décrit comment gérer les utilisateurs dans NetWitness Suite à l'aide de rôles et d'autorisations. Disponible dans le

Guide de la sécurité du système et de la gestion des utilisateurs > Gérer les utilisateurs à l'aide de rôles et d'autorisations.

Accéder à la Gestion de la source d'événements

Pour afficher les détails de vos groupes de sources d'événement existants, procédez comme suit :

1. Accédez à **ADMIN > Sources d'événements**.



2. Cliquez sur l'une des options suivantes :
   - Onglet **Découverte**. Utilisez cet onglet pour consulter les types de sources d'événements que NetWitness a découvert pour chaque adresse ainsi que le degré de fiabilité avec lequel ils ont été identifiés selon le système.
   - Onglet **Gérer**. Cet onglet affiche les détails de vos groupes de sources d'événement existants.
   - Onglet **Politiques de surveillance**. Utilisez cet onglet pour afficher ou modifier la configuration des alertes pour vos sources d'événement.

- Onglet **Alarmes** . Utilisez cet onglet pour afficher les détails des alarmes générées. Les alarmes sont générées lorsque les sources d'événements sont supérieures ou inférieures aux seuils définis.
- Onglet **Paramètres**. Utilisez cet onglet pour afficher ou modifier le comportement des alertes automatiques.

Remarque : Lorsque le système reçoit des logs d'une source d'événement qui n'existe pas actuellement dans la liste Source d'événement, NetWitness Suite ajoute automatiquement la source d'événement à la liste. En outre, si elle répond aux critères d'un groupe existant, elle devient partie intégrante de ce groupe.

Mode de fonctionnement des alarmes et notifications

Le module Source d'événement dans NetWitness Suite affiche les alarmes et envoie des notifications en fonction des alarmes déclenchées.

En matière d'alarmes, tenez compte de ce qui suit :

Les alarmes sont de deux types : **automatiques** (déclenchées lorsque les valeurs de base sont dépassées ou non respectées) et **manuelles** (configurées à l'aide des seuils).

- **Automatique** : Si vous activez les alertes automatiques, le système émet des alarmes pour **toutes** les sources d'événements qui dépassent ou n'atteignent pas leurs valeurs de base normales. Vous pouvez spécifier le pourcentage de dépassement ou restant à atteindre sous l'Onglet Paramètres.
- **Manuel** : Si vous désactivez les alertes automatiques, vous recevez des alarmes uniquement pour les groupes de sources d'événements pour lesquels vous avez spécifié -et activé- des politiques (et des seuils).
- Les alarmes apparaissent dans l'interface utilisateur, sous l'Onglet Alarmes.

En matière de notifications, tenez compte de ce qui suit :

- Pour recevoir des notifications manuelles (par email, SNMP ou Syslog) :
  - Spécifiez une politique pour un groupe de sources d'événements.
  - Définissez un seuil supérieur ou inférieur (ou les deux).
  - Activez la politique.
- Pour recevoir des notifications automatiques (de base) :

- Les alertes de base doivent être activées. Elles sont activées par défaut.
- Vous devez activer les notifications à partir de la surveillance automatique. Pour plus d'informations, reportez-vous à Configuration des alertes automatiques.
- La source de l'événement qui déclenche l'alarme doit faire partie d'un groupe pour lequel une politique est activée.

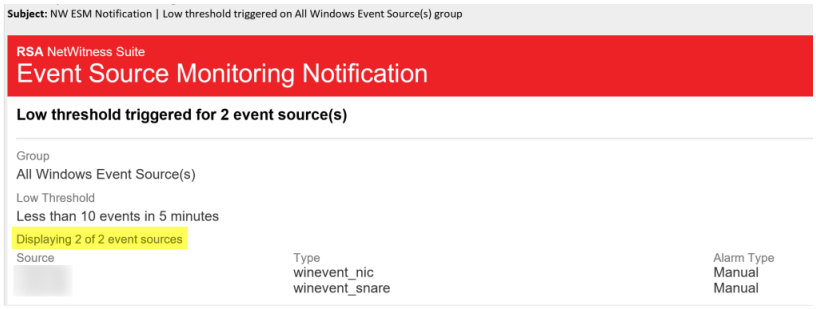
- Si les alertes automatiques sont activées, et si vous avez configuré une politique et un seuil pour un groupe :
  - Si la source de l'événement dépasse sa valeur de base, une alerte automatique s'affiche et vous recevez une notification.
  - Si la source de l'événement dépasse ses seuils, une alerte manuelle s'affiche et vous recevez une notification.
  - Si les deux cas de figure se produisent (dépassement ou non- respect du seuil et de la valeur de base), deux alarmes sont émises (visibles sous l'onglet Alarmes), accompagnées d'une notification. Cette notification répertorie la source de l'événement à l'origine de la double alarme, dont l'une est signalée comme étant une alarme automatique.

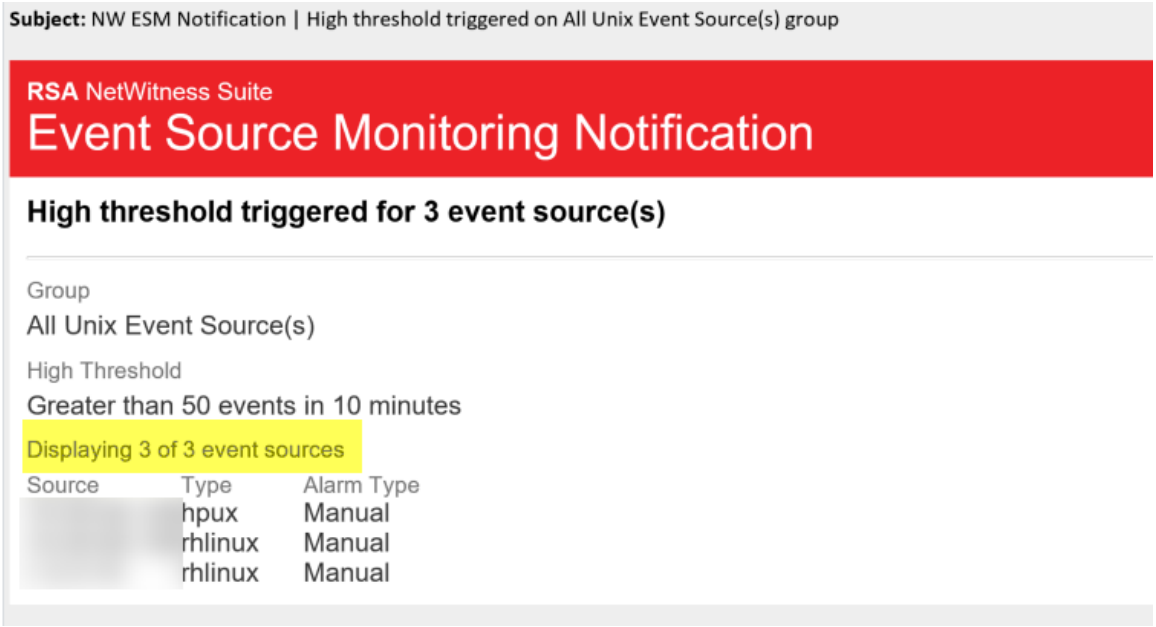
Notifications par e-mail volumineuses

Si vous avez configuré des notifications par e-mail, n'oubliez pas que l'e-mail peut devenir très volumineux, en fonction du nombre de sources d'événements dans la notification.

Si le nombre de sources d'événements dans l'état d'alarme dépasse 10 000, la notification par e-mail contient les détails des 10 000 premières sources et un nombre total. Ceci permet de garantir que l'e-mail est livré correctement.

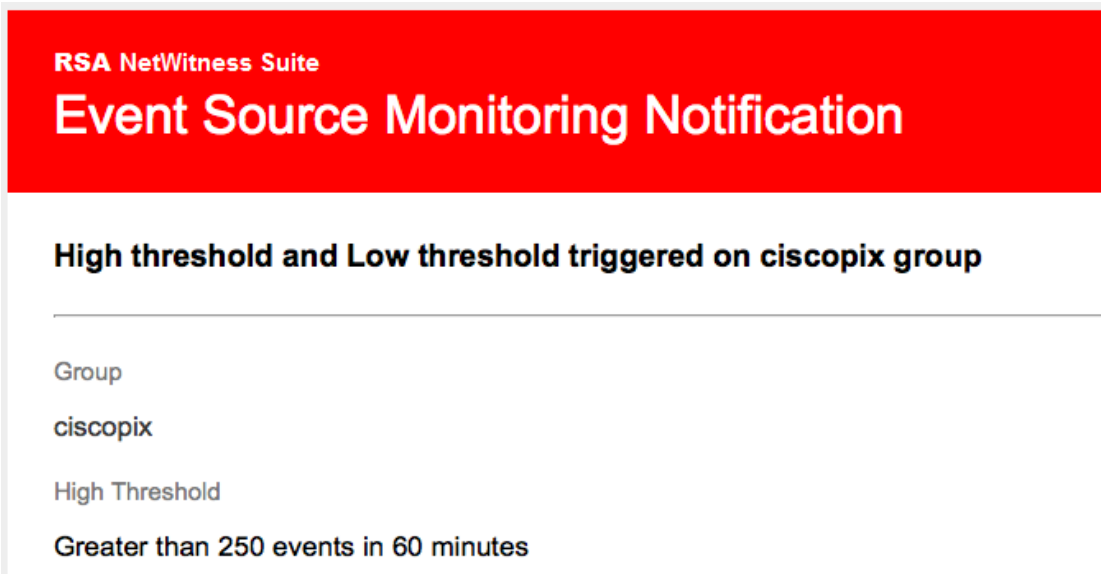
Les exemples suivants montrent deux groupes de sources d'événements ne respectant pas un seuil inférieur et trois groupes de sources d'événements dépassant un seuil supérieur.





Déclenchement des seuils haut et bas

Dans certaines occasions, les alarmes hautes et basses sont toutes deux déclenchées pour un groupe de source d'événement particulier. La meilleure façon de voir quand cela se produit est de lire l'en-tête de l'e-mail, qui indique clairement lorsque les deux seuils sont déclenchés, comme le montre cette image :



Dans cet exemple, l'en-tête indique « High threshold and Low threshold triggered on ciscopix group » (Seuil inférieur et seuil supérieur déclenchés sur le groupe ciscopix). Pour voir les détails des sources d'événements avec des seuils bas, vous devrez peut-être faire défiler des centaines, voire des milliers, de sources d'événements de seuils hauts passées.

Alertes automatiques

Cette rubrique décrit les alertes automatiques qui sont configurées en fonction des paramètres de base.

Remarque : La configuration d'une alerte automatique et de tous les paramètres qui déterminent son comportement, sont actuellement au stade de test Bêta.

Vous pouvez définir des règles et des seuils pour vos groupes de sources d'événements afin de recevoir des notifications lorsque les seuils ne sont pas respectés. NetWitness Suite fournit aussi un moyen automatique de recevoir des alarmes si vous ne souhaitez pas configurer des seuils au delà desquels générer des alarmes.

Pour déclencher des alertes automatiques, vous pouvez utiliser les valeurs de base. Ainsi, vous n'avez pas besoin de configurer de nombreux seuils de groupe ni un tas de règles en vue de recevoir ces alertes. Une quantité anormale de messages suffit à provoquer le déclenchement des alertes, sans avoir à effectuer une configuration particulière (sauf pour activer une alerte automatique).

Notez les points suivants :

- Dès que vous commencez à collecter des messages provenant d'une source d'événement, il faut environ une semaine pour que le système puisse stocker une valeur de référence pour cette source d'événement. Après cette période initiale, le système vous avertit lorsque le nombre de messages sur une période est supérieur ou inférieur à la ligne de base pour une quantité donnée. Par défaut, cette quantité correspond à un écart-type de 2 au-dessus ou en dessous de la ligne de base.
- Basez vos paramètres d'écarts supérieur et inférieur sur la « régularité » du comportement de vos sources d'événements. Autrement dit, si vous vous attendez à peu ou pas de variation dans le nombre de messages qui arrivent pendant une période donnée (par exemple, entre 08:00 et 09:00 un jour de semaine), vous pouvez définir une valeur faible pour l'écart. Inversement, si vous constatez souvent des pics et des creux, vous pouvez définir une valeur d'écart supérieure.
- Si vous activez une règle sans avoir de seuil défini, vous continuerez à recevoir des notifications automatiques (de base) tant que l'alerte automatique est activée.

Scénarios communs pour les politiques de surveillance

Généralement, les organisations doivent surveiller leurs sources d'événements dans des « buckets » basés sur le niveau de criticité des sources d'événements. Voici un exemple typique :

- Il existe un groupe d'appareils PCI, et il est essentiel de savoir si l'un de ces appareils cesse d'envoyer des messages (ou envoie trop peu de messages) sous une demi-heure.
- Il existe un groupe d'appareils Windows, et il est utile de savoir si l'un de ces appareils cesse d'envoyer des messages après quatre heures.
- Il existe un groupe d'appareils silencieux qui n'envoient généralement pas beaucoup de messages, mais vous souhaitez savoir s'ils n'envoient rien pendant 24 heures.

De nombreuses organisations pourraient avoir un réseau qui ressemble à cet exemple. Vous pouvez avoir plusieurs catégories ou elles peuvent être différentes, mais nous utiliserons cet exemple pour aborder le mode d'utilisation de cette fonction.

Vous pouvez avoir des dizaines, voire des centaines de groupes de sources d'événements, mais n'avoir que quelques groupes pour lesquels vous avez besoin de définir des seuils et des alertes.

Remarque : Si une source d'événement est un membre de plusieurs groupes sur lesquels l'alerte est configurée, il n'alertera que le premier groupe correspondant dans la liste classée. (L'onglet Politiques de surveillance présente une liste classée de vos groupes.)

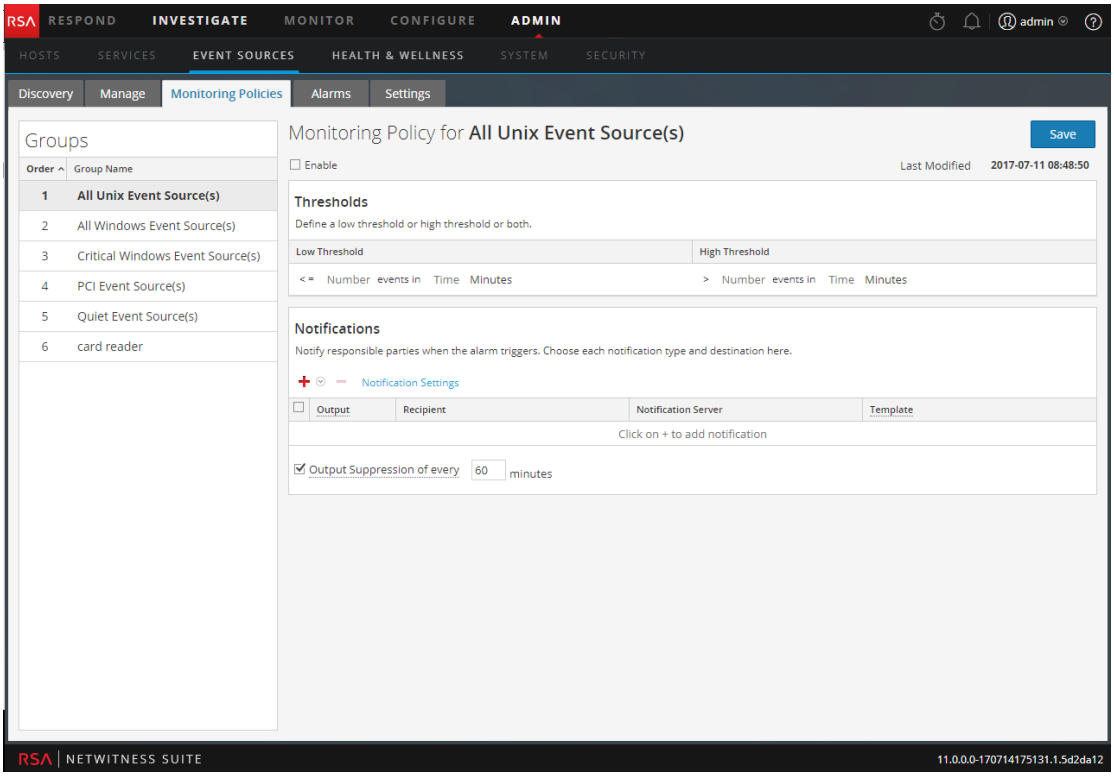
Classement des groupes

Remarque : Pour modifier l'ordre des groupes, glissez -déplacez un groupe vers son nouvel emplacement. Les groupes placés en tête de liste sont prioritaires sur ceux qui suivent : RSA NetWitness Suite vérifie les seuils dans l'ordre prévu dans ce panneau. Ainsi, vos groupes prioritaires doivent être en haut de cette liste.

La première chose à garder à l'esprit est la façon dont vous classez vos groupes sur la page Politiques de surveillance. Si vous possédez les trois groupes mentionnés ci-dessous, vous devez les classer comme suit :

1. Sources d'événements silencieuses. Le fait de posséder ce groupe permet de s'assurer que vous n'obtiendrez pas beaucoup de fausses alertes.
2. sources d'événements PCI à priorité élevée. Les appareils à priorité supérieure doivent se trouver après les appareils silencieux
3. Sources d'événements Windows. La période est plus longue (quatre heures contre une demi-heure) pour ces appareils par rapport aux appareils PCI. Ils doivent donc être placés après les appareils PCI.
4. Toutes les sources d'événements. Vous pouvez éventuellement définir des seuils pour tous les appareils en tant qu'interception globale. Ceci permet de s'assurer que tout votre réseau fonctionne tel que vous l'attendez. Pour le groupe « fourre-tout », inutile de spécifier des seuils d'alerte : vous pouvez utiliser l'alerte automatique pour générer des alarmes pour les

sources d'événements de ce groupe.



Dans la figure ci-dessus, notez ce qui suit :

- Les groupes sont classés comme indiqué dans la section précédente.
- Le seuil des appareils PCI a pour but d'alerter si le nombre de messages entrants dans NetWitness Suite est inférieur à 10 messages en 30 minutes.
- Un seuil inférieur est défini, mais pas un seuil supérieur. Ceci est classique pour de nombreux cas d'utilisation.

Après avoir configuré et classé vos groupes et commencé à recevoir des alertes, vous pouvez avoir à ajuster l'ordre. Utilisez ces instructions pour ajuster l'ordre :

- Si vous recevez trop de notifications, vous pouvez descendre le groupe dans l'ordre. De même, si vous recevez trop peu de notifications, vous pouvez déplacer le groupe vers le haut.
- Si vous notez qu'une source d'événement crée plus d'alertes qu'elle ne le devrait, vous pouvez la déplacer dans un autre groupe ou créer un nouveau groupe pour cette source d'événement.

Gestion des groupes de sources d'événements

Définitions

Lorsque vous utilisez des groupes de sources d'événements dans NetWitness Suite, tenez compte des points suivants :

- Une **source d'événements** est essentiellement une combinaison des valeurs de tous ses attributs.
- Un **groupe de source d'événements** regroupe l'ensemble des sources d'événements qui correspondent aux critères définis pour ce groupe.

Par exemple, vous pouvez utiliser les groupes suivants :

- Groupe **Périphériques Windows**, qui regroupe tous les types de sources d'événements associés aux sources d'événements Microsoft Windows (`winevent_nic`, `winevent_er` et `winevent_snare`).
- Groupe **Services à faible priorité**, qui regroupe tous les services dans lesquels l'attribut Priorité est paramétré sur une valeur inférieure à 5.
- Groupe **Serveurs commerciaux français**, qui regroupe toutes les sources d'événements situées en France et dont l'attribut Organisation est Ventes, Finance ou Marketing.

Détail de l'onglet Gérer

L'onglet Gérer du module Sources d'événements permet de gérer facilement les sources d'événements. Dans cet onglet, vous pouvez :

- Définir des groupes de sources d'événements de façon homogène
- Utiliser des attributs de sources d'événements de façon simple et homogène
- Rechercher facilement des sources dans un ensemble de sources d'événements
- Modifier et mettre à jour en bloc les sources d'événements et les groupes de sources d'événements

Vous pouvez consulter le détail des groupes de sources d'événements en procédant comme suit :

1. Accédez à **Administrateur** > **Sources d'événements**.
2. Sélectionnez le panneau **Gérer** pour consulter le détail de vos groupes de sources d'événements.

Remarque : Lorsque le système reçoit des logs d'une source d'événement qui n'existe pas actuellement dans la liste Source d'événement, NetWitness Suite ajoute automatiquement la source d'événement à la liste. Par ailleurs, si elle répond aux critères d'un groupe existant, elle devient partie prenante de ce groupe.

Groupes par défaut

RSA NetWitness Suite comprend plusieurs groupes par défaut. Vous pouvez personnaliser ces groupes selon vos besoins et vous en servir comme modèles pour créer d'autres groupes.

Les groupes par défaut sont les suivants :

- Toutes les sources d'événements
- Toutes les sources d'événements Unix
- Toutes les sources d'événements Windows
- Sources d'événements Windows critiques
- Sources d'événements PCI
- Sources d'événements silencieuses

Vous pouvez modifier n'importe lequel de ces groupes pour rechercher les règles qui les définissent.

Remarque : Vous ne pouvez pas modifier ni supprimer le groupe **Toutes** les sources d'événements.

Création de groupes de sources d'événements

Les administrateurs doivent recevoir des notifications lorsque les sources d'événements ne sont plus collectées par NetWitness Suite. Ils doivent pouvoir configurer la durée pendant laquelle les sources d'événements peuvent rester silencieuses (noneollecte de messages log) avant d'envoyer une notification basée sur différents facteurs.

RSA NetWitness Suite fournit des groupes de sources d'événements pour que vous puissiez regrouper des appareils d'importance similaire. Vous pouvez créer des groupes d'après les attributs que vous avez importés à partir de votre CMDB (base de données de gestion de configuration), ou en choisissant manuellement les sources d'événements à ajouter au groupe.

Par exemple, voici quelques-uns des types de groupes de source d'événement que vous pouvez créer :

- Source PCI
- Contrôleurs de domaine Windows

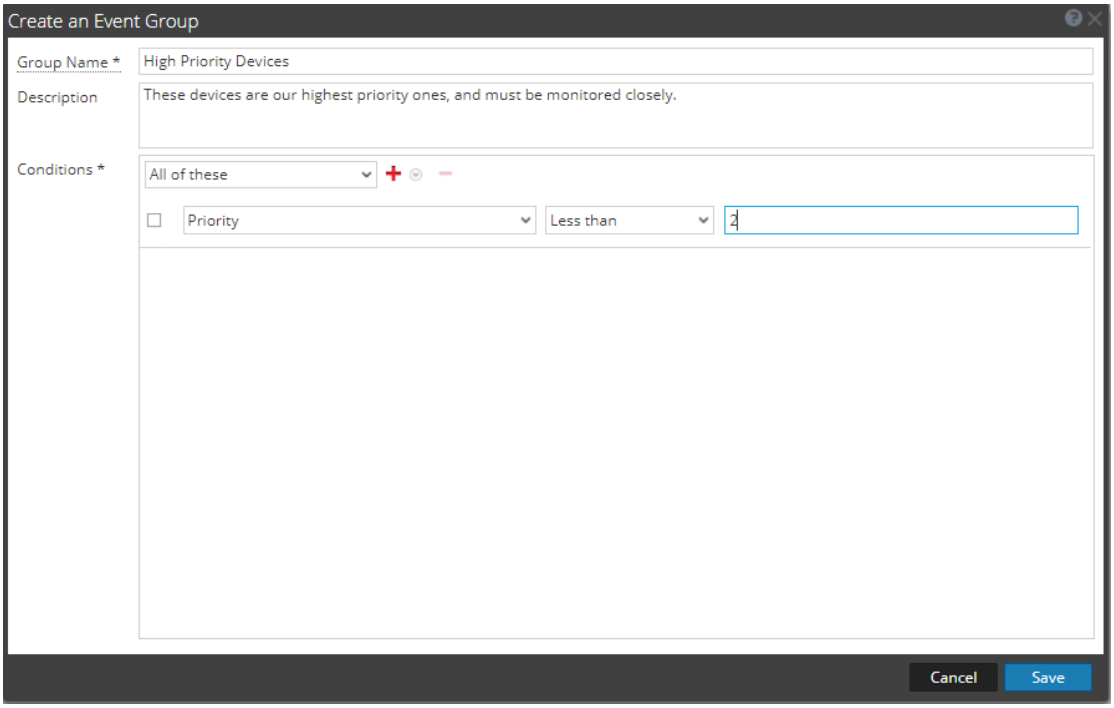
- Sources silencieuses
- Serveurs de finance
- Appareils haute priorité
- Toutes les sources Windows

Procédure

Pour créer un groupe de source d'événement :

1. Accédez à **Administrateur > Sources d'événement**.
2. Dans le panneau **Gérer**, cliquez sur +.

   La boîte de dialogue Créer un groupe d'événements s'affiche.



3. Saisissez un nom de groupe.
4. Saisissez une description.
5. Cliquez sur + pour ajouter une condition. Continuez d'ajouter des conditions selon le besoin. Pour plus de détails sur les conditions de construction, voir Créer/modifier un formulaire de groupe.
6. Cliquez sur **Enregistrer**.

   Le nouveau groupe est indiqué dans le panneau **Gérer**.

Exemples

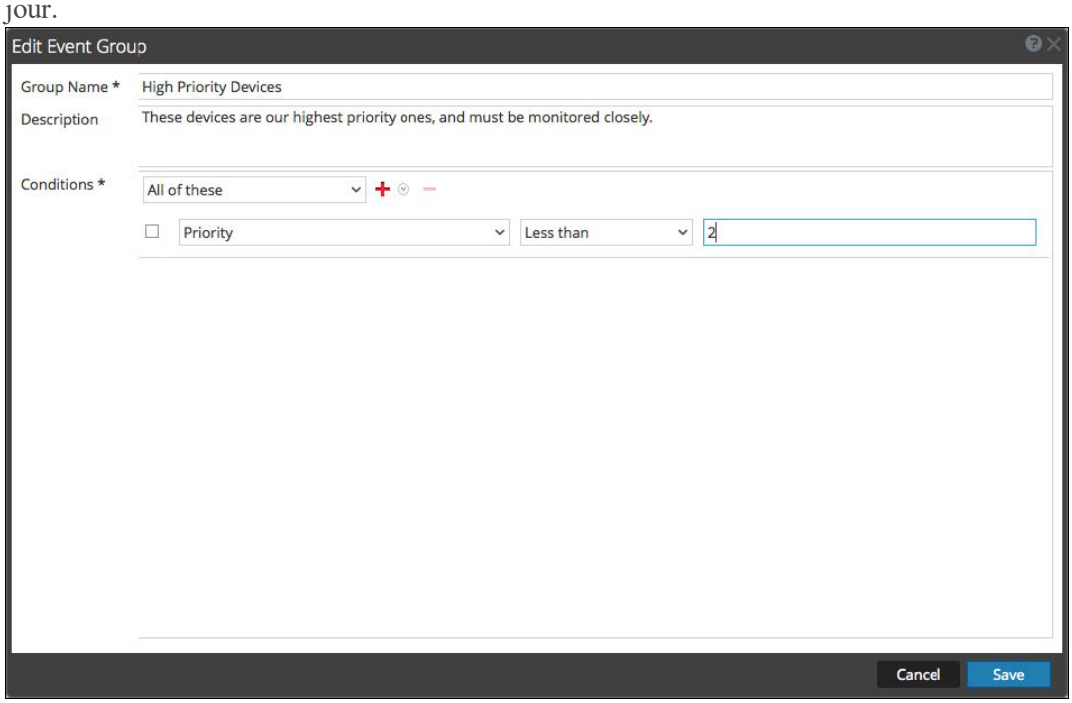
Cette section décrit un exemple isolé, puis indique comment configurer un groupe de règles plus complet.

Exemple isolé

Si vous souhaitez créer un groupe de sources d'événements qui contient toutes vos sources d'événements haute priorité, cet exemple décrit les étapes nécessaires.

1. Accédez à **Administrateur > Sources d'événements**.
2. Dans le panneau **Gérer > Groupes**, cliquez sur +.
3. Saisissez **Appareils haute priorité** pour le nom du groupe.
4. Saisissez une description, telle que « Ces appareils sont notre première priorité et doivent être étroitement surveillés. »
5. Laissez **Tous** sélectionné et cliquez sur + pour ajouter une condition.
6. Sélectionnez **Ajouter une condition** dans le menu déroulant.
   a. Sélectionnez un attribut : **Priorité**.
   b. Sélectionnez un opérateur : **Inférieur à**.
   c. Saisissez une valeur : **2.**

   La figure suivante affiche la boîte de dialogue Modifier le groupe d'événements mise à jour.



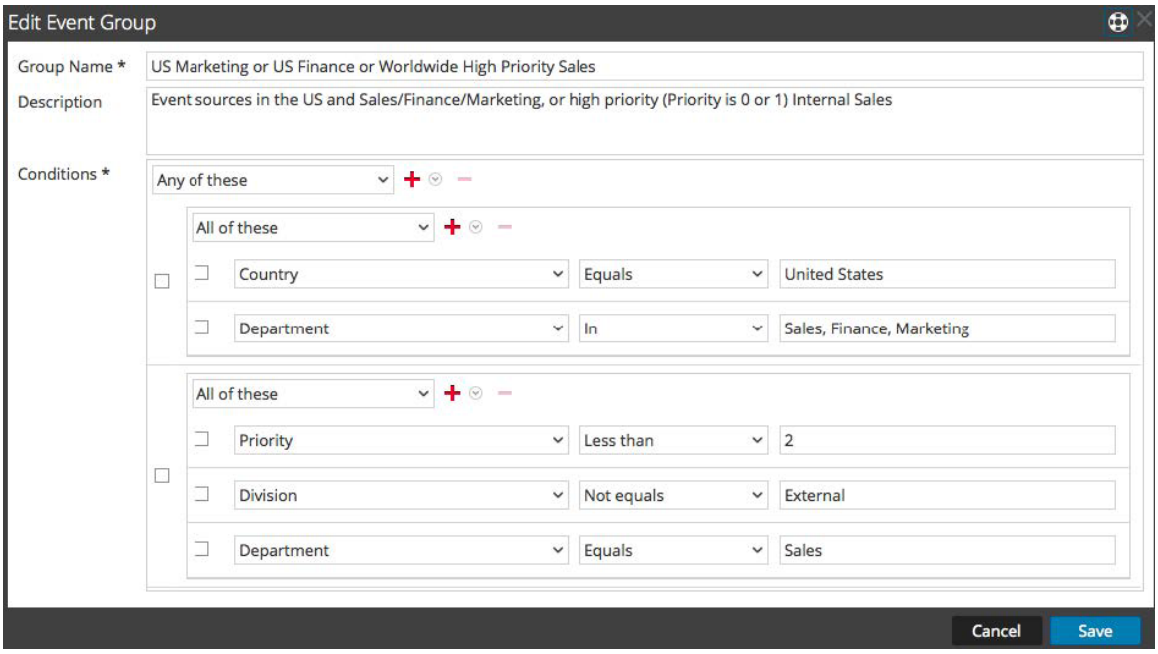
7. Cliquez sur **Enregistrer**.

Exemple complexe

Dans cet exemple, vous devez créer une règle assez complexe : associer des sources d'événements qui sont aux États-Unis et dans les services Ventes, Finance ou Marketing. De même, associez des sources d'événements de ventes internes et haute priorité dans le monde entier. Une priorité élevée doit être attribuées aux priorités 1 ou 0. Logiquement, la définition est la suivante :

```
(Country=United States AND (Dept.=Sales OR Dept.=Finance OR
Dept.=Marketing))
 OR
 (Priority < 2 AND Division != External AND Dept.=Sales)
```

La figure suivante est un exemple de critères de création d'un groupe de sources d'événements.



Formulaire de création de groupes de sources d'événements

Le formulaire Créer des groupes de sources d'événements s'affiche lorsque vous créez ou modifiez un groupe de sources d'événements.

Paramètres

Le tableau suivant décrit les champs du formulaire Modifier/créer un groupe d'événements.

Champ	Description
Nom du groupe	Ce champ est obligatoire et s'affiche via l'interface utilisateur de NetWitness Suite en tant qu'identifiant du groupe.
Description	Description facultative permettant de décrire l'objectif ou les détails du groupe.
Outils 	Les éléments suivants sont disponibles dans la barre d'outils : • **Ajouter (+)** : cliquer sur **Ajouter** affiche un menu dans lequel vous pouvez choisir d'ajouter une condition ou un groupe. • **Supprimer (−)** : supprime la règle ou le groupe de règles sélectionné de la liste. Lorsque vous ajoutez un nouveau groupe, des niveaux imbriqués de conditions sont également créés.
Conditions	Décrites ci-dessous dans le tableau **Critères de règle**.
Annuler / Enregistrer	Les options **Annuler** et **Enregistrer** sont disponibles dans le formulaire.

Critères de règle

Les règles que vous spécifiez déterminent les sources d'événements qui feront partie de ce groupe de sources d'événements. Une règle se compose des éléments suivants :

- Regroupement : comment la règle interagit avec les autres règles
- Attribut : à quel attribut la règle correspond-t-elle
- Opérateur : comment la règle correspond à l'attribut
- Valeur : valeur d'attribut utilisée pour la règle

Le tableau suivant détaille ces constructeurs de règles.

Constructeur de règle	Détails
Groupe	Vous pouvez regrouper les conditions afin de créer des règles complexes pour un groupe de sources d'événements. Les choix suivants sont disponibles lors du regroupement de vos règles : • **Tous** : équivalent logique de AND • **Aucun** : équivalent logique de OR • **Aucun d'entre eux** : équivalent logique de NOT Si vous créez une groupe simple et que vous spécifiez une seule condition, vous pouvez alors conserver la valeur par défaut (**Tous**) sélectionnée.
Attributs	Contient une liste déroulante composée de tous les attributs de sources d'événements. Les attributs s'affichent en fonction de la section à laquelle ils appartiennent. Par exemple, tous les attributs **Identification** s'affichent en premier, suivi de **Propriétés**, **Importance**, etc.

Constructeur de règle	Détails

Opérateur	Choisissez parmi les options suivantes :
	• **Est égal à** : équivaut à la valeur fournie
	• **Différent(e) de** : renvoie des sources d'événement dont l'attribut spécifié n'est pas égal à la valeur fournie
	• **Dans** : fournit une liste de valeurs séparées par des virgules, et des sources d'événement qui correspondent à toutes les valeurs fournies sont incluses. Par exemple :
	`Where IP in 10.25.50.146, 10.25.50.248`
	Cette condition renvoie des sources d'événement qui possèdent `10.25.50.146 or 10.25.50.248` en tant qu'attribut IP.
	• **Pas dans** : semblable à **In**, mais il correspond aux éléments dont l'attribut n'est égal à aucune des valeurs répertoriées.
	• **Semblable à** : correspond aux éléments qui commencent par la chaîne fournie. Par exemple :
	`Where Event Source Type Like Apache`
	Cette condition renvoie des sources d'événements dont le Type de Source événements commence par`Apache`.
	• **Non semblable à** : semblable à **Like**, mais il correspond aux éléments dont l'attribut ne commence pas par la chaîne fournie.
	• **Supérieur(e) à** : correspond aux éléments dont l'attribut est supérieur à la valeur fournie. Par exemple, si vous spécifiez Priorité supérieure à 5, la condition correspondrait à un élément avec une priorité de 6 ou supérieure.
	• **Inférieur(e) à** : semblable à **Supérieur(e) à**. Correspond aux éléments dont l'attribut est inférieur à la valeur fournie.

Valeur	Saisissez une valeur ou un groupe de valeurs. Le type de valeur dépend de l'attribut de la condition. Par exemple, pour IPv6, vous devez spécifier une valeur au format IPv6.

Reconnaissance et mappage des sources d'événements

Reconnaître les types de sources d'événements

L'onglet Découverte vous permet d'examiner les types de source d'événement que NetWitness a découvert pour chaque adresse et le degré de précision avec lequel le système les a identifiés. Si les types de source d'événement découverts sont corrects, vous pouvez reconnaître pour filtrer cette source d'événement à partir de la vue par défaut. S'ils sont incorrects, vous pouvez définir les types de sources d'événements autorisés pour une adresse particulière afin que les futurs logs puissent être analysés par rapport aux parsers corrects.

Pour reconnaître que les types de source d'événement découverts sont corrects, procédez comme suit.

- Sélectionnez les Sources d'événements que vous souhaitez reconnaître, puis cliquez sur le bouton **Reconnaître** dans la barre d'outils. Une fois que les Sources d'événements sont reconnues, elles ne s'affichent plus dans la colonne de Types de sources d'événements.

Remarque : Les sources d'événements reconnues ne sont pas affichées par défaut.

Mapper des types de sources d'événements

Lorsque des types de sources d'événement découverts ne sont pas complètement justes, vous pouvez mapper les parsers pour obtenir des informations supplémentaires en procédant comme suit :

- Sélectionnez les Sources d'événements que vous souhaitez mapper, puis cliquez sur le bouton **Mapper** dans la barre d'outils.

Remarque : Les scores de découverte des sources d'événements mappées sont répertoriés dans la colonne de Types de sources d'événements, du plus bas au plus élevé. Les scores de découverte ont une valeur allant de 0 (score le moins sûr) à 100 (score le plus sûr).

Affichage des logs à partir des versions de Log Decoder antérieures à 11.0.0.0

NetWitness 11.0.0.0 a ajouté la possibilité d'afficher un petit échantillon des logs récents pour certains périphériques via des onglets de détails de la vue Découverte. Par défaut, les versions de Log Decoders antérieures à 11.0.0.0 ne possèdent pas la configuration requise pour activer cette fonction, mais quelques changements mineurs peuvent la rendre disponible.

Pour activer l'aperçu des logs pour une version de Log Decoder antérieure à 11.0.0.0, suivez ces étapes dans le Log Decoder :

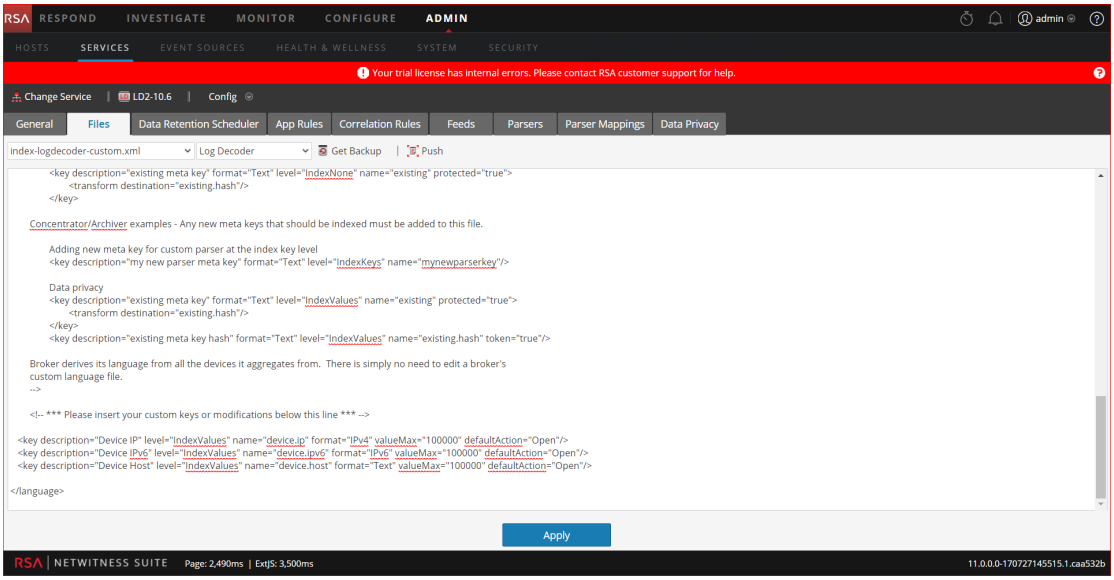
1. Accédez à **ADMIN > Services >**, sélectionnez un Log Decoder, puis > **Vue** > **Config**.
2. Cliquez sur l'onglet **Fichiers**, puis dans le menu déroulant, sélectionnez **index-logdecoder-custom.xml**.
3. Ajoutez les trois lignes suivantes à la fin du fichier (avant la balise de langue fermante) :

```
<key description="Device IP" level="IndexValues" name="device.ip" format="IPv4"
valueMax="100000" defaultAction="Open"/>

<key description="Device IPv6" level="IndexValues" name="device.ipv6" format="IPv6"
valueMax="100000" defaultAction="Open"/>

<key description="Device Host" level="IndexValues" name="device.host" format="Text"
valueMax="100000" defaultAction="Open"/>
```

4. Cliquez sur **Appliquer**.

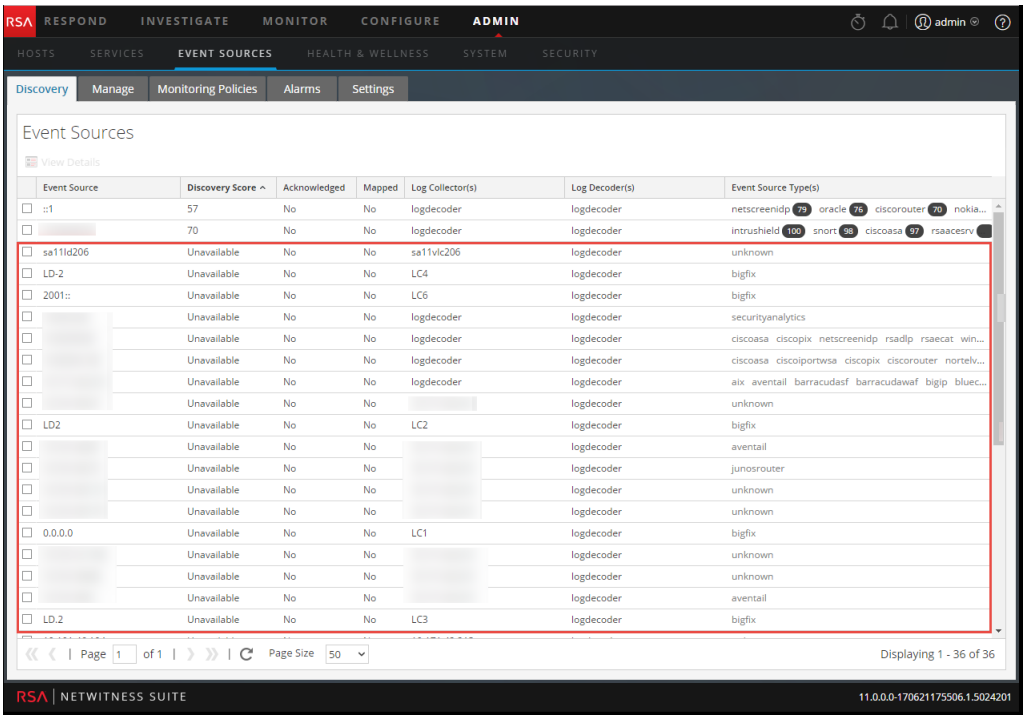


5. Redémarrez le Log Decoder comme suit.
   Sélectionnez **Log Decoder > Explorer > Système > Propriétés > Arrêt**

Exemple de fichier **index-logdecoder-Custom.XML**.

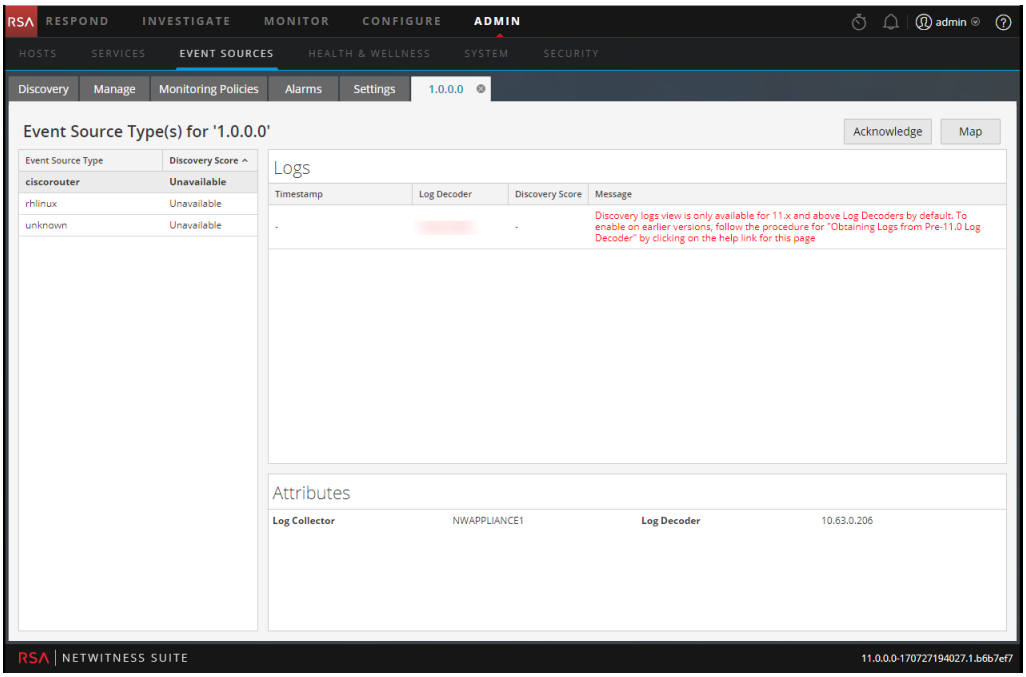
> **Remarque :** Les scores de découverte ne sont disponibles que pour les services Log Decoder 11.0.0.0 et versions ultérieures. Les scores de découverte pour les versions Log Decoders antérieures à 11.0.0.0 s'affichent comme étant non disponibles.

L'exemple suivant affiche un score de découverte considéré comme **Non disponible** dans la vue **Détails** pour une version de Log Decoder antérieure à 11.0.0.0.



Remarque : Les logs de périphériques sont uniquement disponibles pour les versions de Log Decoder 11.0.0.0 et ultérieures.

L'exemple suivant affiche le message qui s'affiche dans le volet Logs pour une version de Log Decoder antérieure à 11.0.0.0.



Modification ou suppression des groupes de sources d'événements

Parfois, vous pouvez avoir besoin de supprimer un groupe de sources d'événements. Par exemple, si vous fermez un bureau et que vous aviez un groupe composé de toutes les sources d'événement dans ce bureau, vous pouvez supprimer ce groupe, car aucune de ces sources d'événements n'enverra d'informations à NetWitness Suite.

De même, vous devrez peut-être modifier certaines des conditions qui sont utilisées pour remplir le groupe.

Remarque : Vous ne pouvez pas modifier le nom du groupe de sources d'événements. Une fois que vous avez créé un groupe, ce nom existe aussi longtemps que le groupe lui-même existe.

Modifier un groupe de sources d'événements

1. Accédez à **Administrateur > Sources d'événements**.
2. Dans le panneau **Gérer**, sélectionnez un groupe de sources d'événements existant.
3. Cliquez sur  .

   La boîte de dialogue Modifier le groupe d'événements s'affiche.
4. Modifiez les détails, ou ajoutez, modifiez ou supprimez les conditions si nécessaire.
5. Cliquez sur **Enregistrer**.

Supprimer un groupe de sources d'événements

Notez les points suivants :

- Vous pouvez supprimer tous les groupes, sauf le groupe **Toutes**, qui énumère toutes les sources d'événements configurées dans le système.
- Si vous supprimez un groupe, la règle associée à ce groupe est également supprimée automatiquement.
- S'il y a des sources d'événements qui appartiennent **uniquement** au groupe supprimé, alors il ne restera plus aucune alarme de la règle qui lui est associée. Rappelez-vous que les sources d'événements peuvent appartenir à plusieurs groupes.
- La suppression d'un groupe n'a pas d'effet sur les alarmes de base.

Pour créer un groupe de sources d'événements :

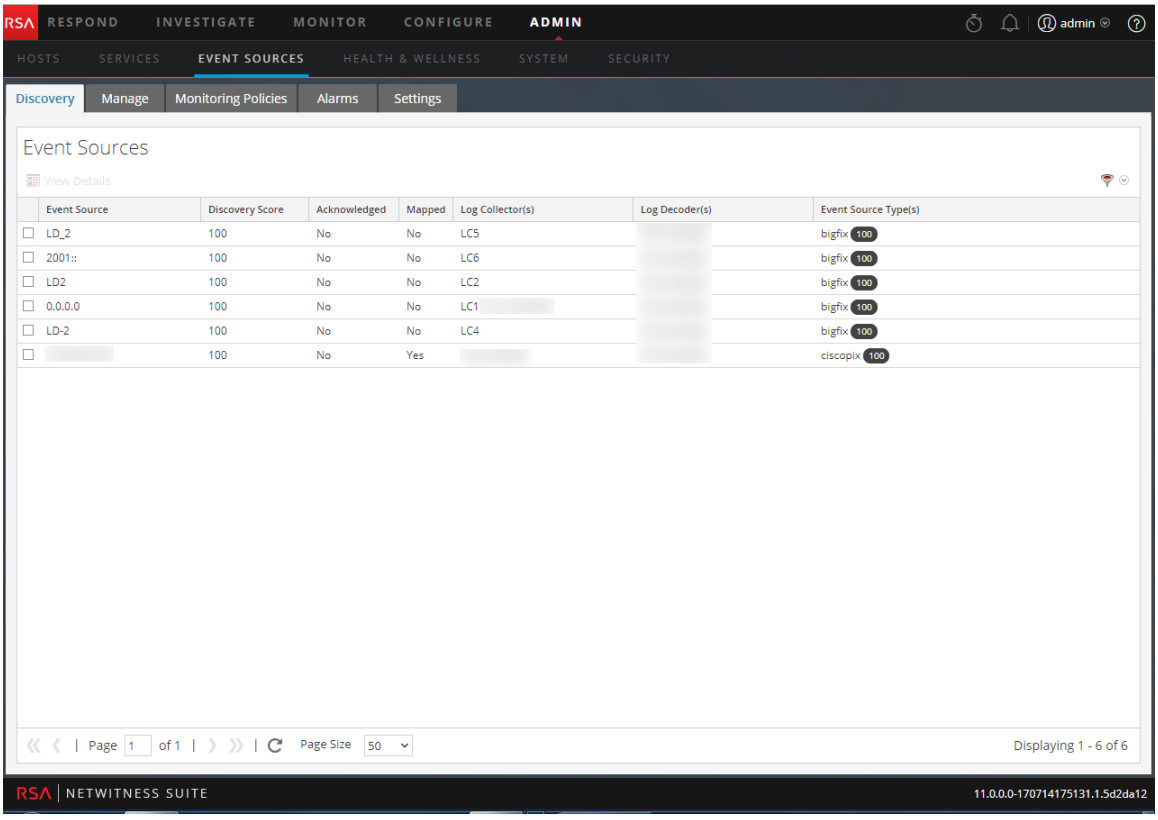
1. Accédez à **ADMIN > Sources d'événements**.
2. Dans le panneau **Gérer**, sélectionnez un groupe de sources d'événements existant.
3. Cliquez sur .

   Une boîte de dialogue de confirmation s'affiche.
4. Cliquez sur **Oui** pour supprimer le groupe.

Création d'une source d'événement et modification des attributs

Vous pouvez organiser vos sources d'événements en groupes. Pour cela, vous devez saisir des valeurs pour différents attributs de chaque source d'événement. Par exemple, pour toutes vos sources d'événements haute priorité, vous pouvez définir la **Priorité** sur 1. Vous pouvez afficher des détails sur les attributs disponibles dans l'onglet Onglet Gérer la source d'événement.

La figure suivante donne un exemple du panneau sources d'événements :



Les attributs de source d'événement sont une association d'informations remplies automatiquement et saisies par l'utilisateur. Lorsqu'une source d'événement envoie des informations de log à NetWitness Suite, elle est ajoutée à la liste de sources d'événement, et certaines informations de base sont remplies automatiquement. À tout moment par la suite, les utilisateurs peuvent ajouter ou modifier des détails pour d'autres attributs de source d'événement.

Attributs obligatoires

Les attributs d'identification suivants sont gérés de manière spéciale : **IP**, **IPv6**, **Nom d'hôte**, **Type de source d'événement**, **Log Collector** et **Log Decoder**. Si vous créez une source d'événement manuellement, vous pouvez saisir ces valeurs. Lorsque vous enregistrez la source d'événement, ces valeurs ne peuvent plus être modifiées.

Les sources d'événements peuvent également être découvertes automatiquement ; toute source d'événement qui envoie des messages au Log Decoder sera ajoutée à la liste de sources d'événements. Si vous modifiez les attributs d'une source d'événement découverte automatiquement, vous ne pouvez modifier aucun de ces champs.

Notez que tous ces champs ne sont pas obligatoires. Pour identifier une source d'événement de manière unique, les informations suivantes sont requises :

- IP ou IPv6 ou Nom d'hôte et
- Type de source d'événement

De plus, RSA NetWitness Suite utilise une hiérarchie pour IP, IPv6 et le Nom d'hôte. L'ordre est le suivant :

1. IP
2. IPv6
3. Nom de l’hôte

Si vous saisissez des sources d'événements manuellement, vous devez garder cet ordre à l'esprit. Sinon, des réplicas risquent d'être créés lors de la réception de messages provenant de sources d'événements que vous avez ajoutées manuellement.

Tous les autres attributs (tels que Priorité, Pays, Entreprise, Fournisseur, etc.) sont facultatifs.

Créer une source d'événements

1. Accédez à **Administrateur > Sources d’événements**.
2. Sélectionnez l'onglet **Gérer**.
3. Dans le panneau **sources d'événements**, cliquez sur  pour ouvrir l'écran des détails, qui contient tous les attributs de source d'événement.

   L'onglet Onglet Gérer la source d'événement s'affiche.
4. Saisissez ou modifiez les valeurs pour tous les attributs.
5. Cliquez sur **Enregistrer**.

Mettre à jour les attributs pour une source d'événement

1. Accédez à **ADMIN > Sources d'événements**.
2. Sélectionnez l'onglet **Gérer**.
3. Dans le panneau **sources d'événements**, sélectionnez une source d'événement dans la liste.
4. Dans le panneau **sources d'événements**, cliquez sur  pour ouvrir l'écran des détails, qui contient tous les attributs de source d'événement.

   L'onglet Onglet Gérer la source d'événement s'affiche.
5. Saisissez ou modifiez les valeurs de tous les attributs, à l'exception de certains attributs qui ne peuvent pas être modifiés une fois saisis.
6. Cliquez sur **Enregistrer**.

Modification en bloc de la source d'événement

Vous pouvez sélectionner plusieurs sources d'événements, un groupe de sources d'événements ou l'ensemble de ces sources pour les modifier en bloc. Ce peut être le cas, par exemple, si vous souhaitez modifier la priorité ou le responsable d'un grand nombre de sources d'événements.

Remarque : Vous ne pouvez pas sélectionner des sources d'événements sur les différentes pages affichées. Par exemple, si un groupe comporte 225 sources d'événements et que la taille de pages est limitée à 50, vous pouvez sélectionner les sources d'événements uniquement parmi les 50 éléments affichés.

Pour modifier des éléments couvrant plusieurs pages, procédez comme suit :

- Dans le navigateur, augmentez la taille de page (la valeur maximum est de 500 entrées sur une même page). Si la taille de page est petite, vous pouvez afficher tous vos éléments sur une même page.
- Créez un groupe de sources d'événements contenant uniquement les éléments à modifier en bloc. Ensuite, sélectionnez l'ensemble des éléments du groupe et non quelques-uns uniquement.
- Modifiez les éléments en bloc de façon incrémentielle. Sur la première page, sélectionnez les éléments que vous souhaitez modifier. Apportez les modifications nécessaires, puis accédez à la page suivante. Répétez alors la procédure jusqu'à ce que vous ayez apporté toutes les modifications voulues.

Modifier les attributs en bloc

Remarque : Les champs obligatoires ne peuvent pas être modifiés : IP, IPv6, Nom d'hôte, Type de source d'événements, Log Collector et Log Decoder.

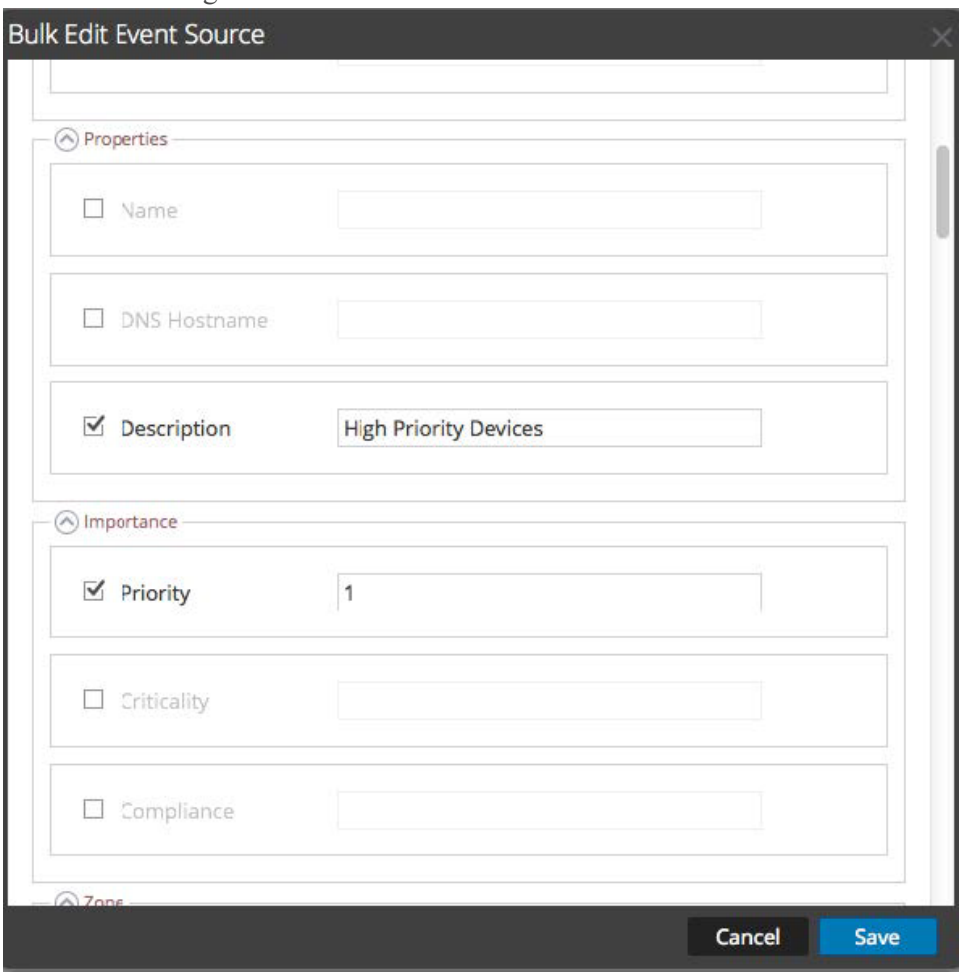
Pour modifier en bloc les attributs des sources d'événements :

1. Accédez à **ADMIN > Sources d'événements**.
2. Sélectionnez l'onglet **Gérer**.
3. Vous pouvez sélectionner un groupe de sources d'événements.
4. Dans le panneau **Sources d'événements**, sélectionnez la ou les sources d'événements à modifier.

   Remarque : Pour sélectionner toutes les sources, cochez la case située à côté de la colonne **Actions** dans la colonne située à l'extrême droite du tableau.

5. Cliquez sur l'icône **Modifier** de la barre de menus.

   La boîte de dialogue Modification en bloc de la source d'événement s'affiche.



6. Saisissez les valeurs des attributs disponibles. Sur la capture d'écran précédente, les attributs de nom et de priorité ont été mis à jour.
7. Une fois les attributs voulus mis à jour, cliquez sur **Enregistrer**.

Importation de sources d'événement

Vous pouvez importer les attributs d'une source d'événement à partir d'un fichier formaté CSV. Pour importer des informations à partir d'une base de données de gestion de configuration (CMDB), une feuille de calcul, ou tout autre type de fichier, convertissez ou enregistrez au préalable les informations dans un fichier CSV.

Remarque : Les attributs d'identification suivants sont gérés de manière spéciale : **IP**, **IPv6**, **Nom d'hôte**, **Type de source d'événement**, **Log Collector** et **Log Decoder**. Si vous importez une source d'événement qui inclut une valeur différente pour un de ces champs (en comparaison avec la valeur dans NetWitness Suite), la valeur d'origine dans NetWitness Suite ne sera **pas** remplacée.

Les attributs importés sont associés à la source d'événement correspondante et sont disponibles pour une utilisation avec les règles afin de créer des groupes de sources d'événements.

RSA NetWitness Suite traite le fichier d'importation comme un dossier complet correct. Cette hypothèse conduit aux comportements suivants liés à l'importation des attributs de sources d'événements :

- Par défaut, lorsque vous importez des attributs, le système met uniquement à jour les attributs des sources d'événements existantes.
- Si la source d'événement existe dans le fichier d'importation, mais pas dans NetWitness Suite, les attributs de cette source d'événement sont ignorés. Autrement dit, NetWitness Suite ne crée **pas** de nouvelle source d'événement pour ces attributs.
- Si la source d'événement existe dans le fichier d'importation et NetWitness Suite, les valeurs de cette source d'événement sont remplacées.
- Si un attribut est vide dans le fichier d'importation, il efface l'attribut correspondant dans NetWitness Suite.
- Si aucun attribut n'est spécifié dans le fichier d'importation, alors l'attribut correspondant est ignoré dans NetWitness Suite (mais il n'est **pas** effacé).

Remarque : Il existe une différence entre un attribut vide et un attribut non spécifié du tout. Si un attribut est spécifié, mais vide, on suppose qu'il est censé être vide ; NetWitness Suite efface alors cet attribut pour la source d'événement correspondante. En revanche, si aucun attribut n'est spécifié du tout, on suppose qu'aucun changement n'est prévu.

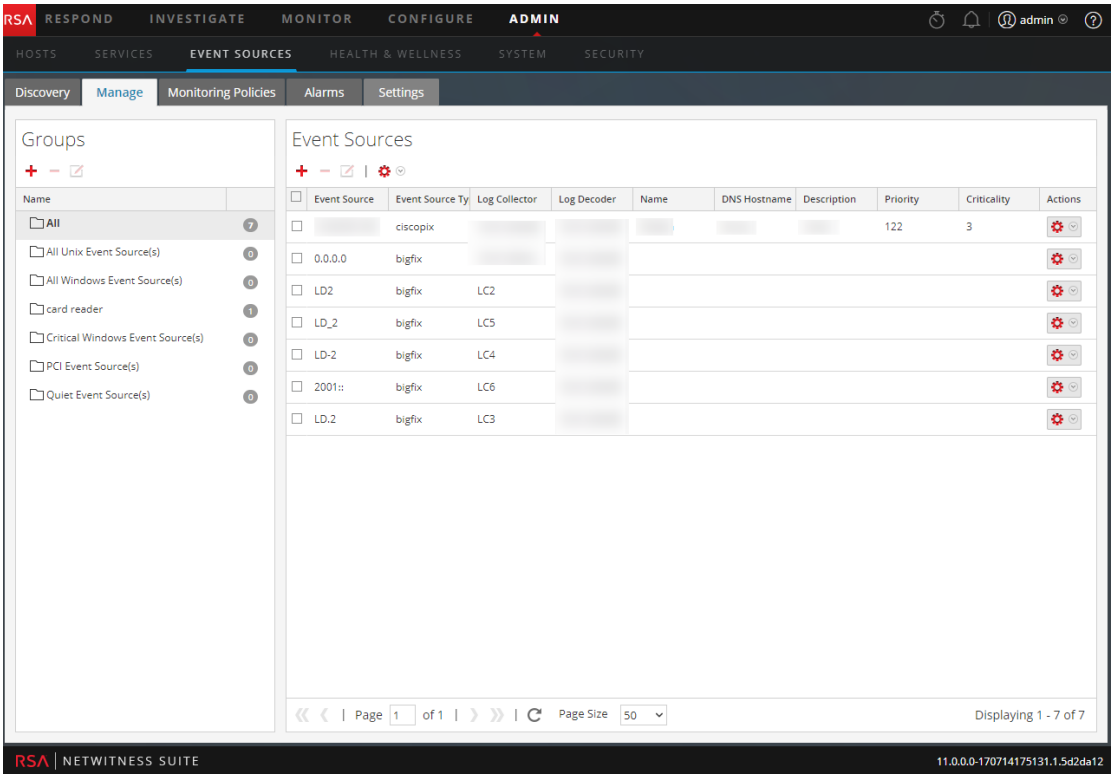
Les comportements ci-dessus correspondent à la configuration par défaut — vous pouvez néanmoins les modifier comme spécifié dans la procédure suivante.

Importer les attributs de source d’événement

Pour importer les attributs d'une source d'événement à partir d'un fichier :

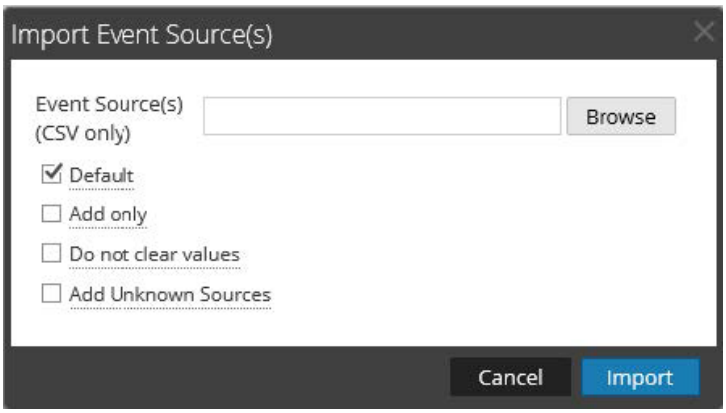
1. Accédez à **Administrateur > Sources d’événements**.
2. Sélectionnez l'onglet **Gérer**.

   L'onglet Gérer les sources d’événements s'affiche.



3. Dans le menu Importer/Exporter de la barre d'outils ( ), sélectionnez **Importer** (Import).

   La boîte de dialogue Importer des sources d'événements s'affiche.



4. Accédez au fichier d'importation, puis sélectionnez les cases appropriées :
   - **Par défaut** : Le comportement par défaut est décrit ci-dessus.
   - **Ajouter uniquement** : Importe un attribut uniquement si le champ correspondant dans NetWitness Suite est vide. Par conséquent, aucune valeur existante n'est pas remplacée.
   - **Ne pas effacer les valeurs** : N'efface pas les valeurs d'attributs dans NetWitness Suite correspondant aux éléments qui sont vides dans le fichier d'importation.
   - **Ajouter des sources inconnues** : Ajoute de nouvelles sources d'événements en fonction des éléments du fichier d'importation.

     Remarque : Vous pouvez sélectionner plusieurs options.
5. Cliquez sur **Importer**.
6. Cliquez sur **Oui** dans la boîte de dialogue de confirmation pour effectuer l'importation.

Dépannage du fichier d'importation

Si votre fichier d'importation n'est pas mis en forme correctement, ou s'il manque des informations requises, un message d'erreur s'affiche et le fichier n'est pas importé.

Vérifiez les éléments suivants :

- Si vous ajoutez des sources inconnues, chaque ligne du fichier devra contenir une combinaison des attributs requis :
  - IP ou IPv6 ou Nom d'hôte et
  - Type de source d'événement
- La première ligne du fichier doit contenir les noms des en-têtes qui doivent correspondre aux noms présents dans NetWitness Suite. Pour obtenir la liste des noms de colonnes corrects,

vous pouvez exporter une seule source d'événement. Examinez le fichier CSV exporté : la première ligne du fichier contient l'ensemble des noms d'attributs/de colonnes appropriés.

Si votre fichier d'importation n'est pas mis en forme correctement, ou s'il manque des informations requises, un message d'erreur s'affiche et le fichier n'est pas importé.

Exportation des sources d'événement

Vous pouvez exporter la totalité ou une partie de vos sources d'événement dans un fichier CSV, accompagnées de leurs attributs correspondants.

Notez les points suivants :

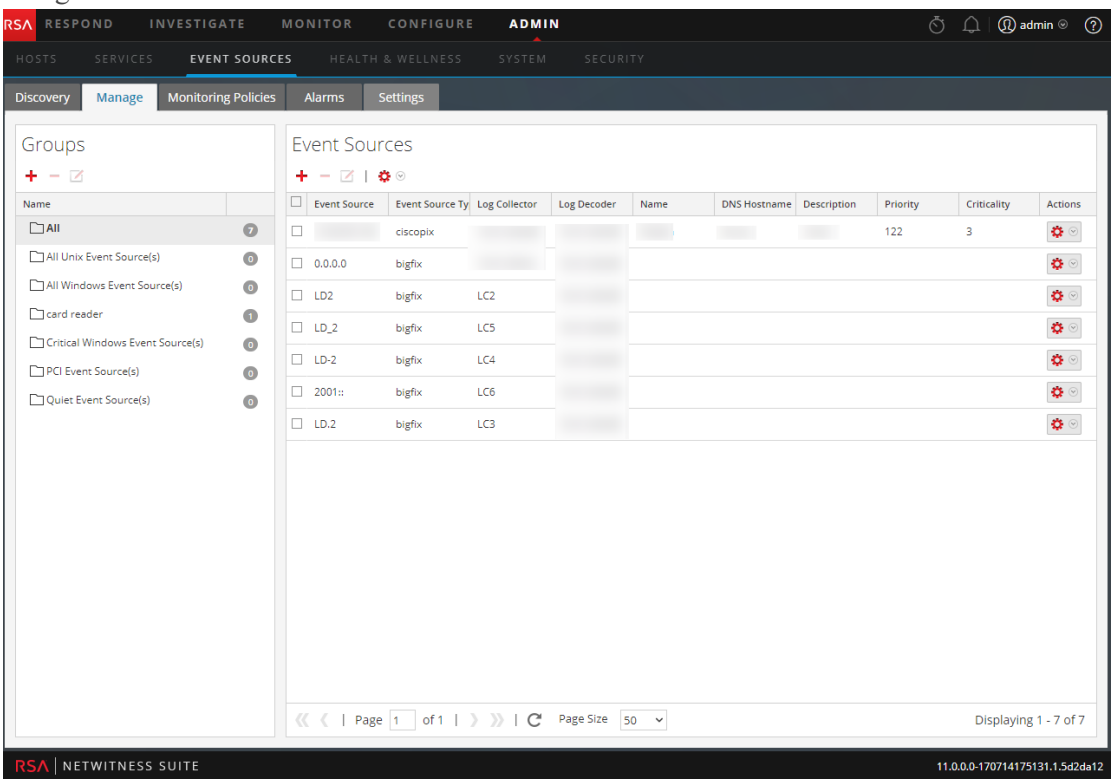
- Le fichier CSV exporté inclut toutes les colonnes d'attributs.
- Le fichier CSV exporté inclut une ligne d'en-tête en haut qui répertorie le nom de chaque colonne.
- Vous pouvez exporter toutes les entrées d'un groupe.
- Vous pouvez exporter toutes les entrées (sélectionnez le groupe **Tous**).
- Vous pouvez sélectionner des entrées et n'exporter que ces entrées.

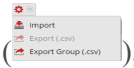
Exporter des sources d'événements

Pour exporter vos sources d'événement :

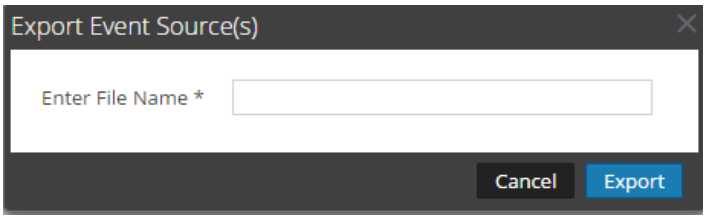
1. Accédez à **Administrateur > Sources d'événements**.
2. Sélectionnez l'onglet **Gérer**.

L'onglet Gérer les sources d'événements s'affiche.



3. Sélectionnez le groupe qui contient les sources d'événement à exporter.
4. Sélectionnez autant de sources d'événement qu'il est nécessaire. Vous pouvez aussi exporter le groupe entier. Pour exporter le groupe entier, il n'est pas nécessaire de sélectionner les différentes sources d'événement.
5. Dans le menu Importer/Exporter de la barre d'outils (), sélectionnez **Exporter (.csv)** ou **Exporter le groupe (.csv)**.

   La boîte de dialogue Exporter des sources d'événements s'affiche.



6. Saisissez un nouveau nom et cliquez sur Export.

Les attributs des sources d'événement sont enregistrés dans le nom de fichier que vous avez spécifié, au format CSV.

Tri des sources d'événement

Le panneau des sources d'événement affiche les attributs du groupe de sources d'événement actuellement sélectionné. Vous pouvez configurer la liste des attributs affichés et aussi trier la liste sur les attributs affichés.

Comportement

Notez les comportements suivants lors du tri des sources d'événement :

- La liste entière est triée et pas seulement les éléments affichés sur la page active. (La barre de navigation au bas de la page affiche le nombre de pages qui existe pour cette liste de sources d'événement.)
- L'ordre de tri est sensible à la casse. Pour toute colonne de chaîne, si les valeurs contiennent une combinaison de minuscules et de majuscules, la majuscule est affichée dans la liste avant la minuscule.

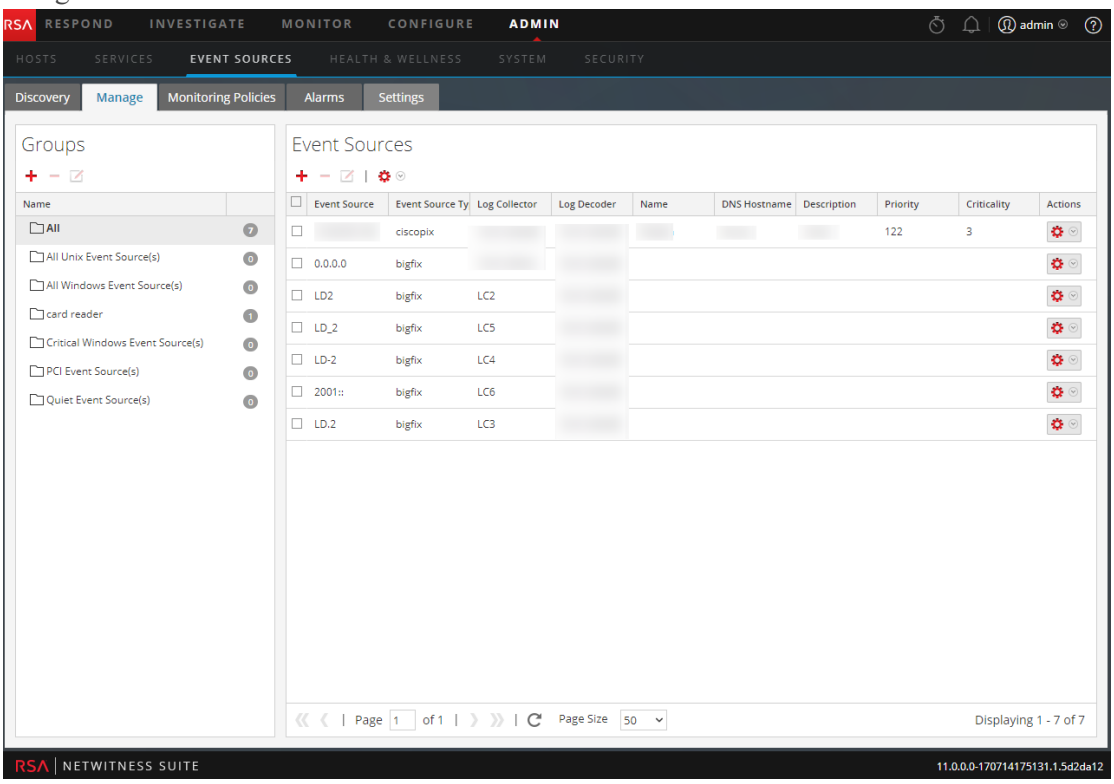
  Par exemple, imaginons que la colonne Type de source d'événement contienne les entrées suivantes : BEDFORD, bangalore, Reston, Londres. L'ordre de tri serait le suivant :

  - BEDFORD
  - bangalore
  - Londres
  - Reston

Pour trier vos sources d'événement :

1. Accédez à **ADMIN > Sources d'événements**.
2. Sélectionnez l'onglet **Gérer**.

L'onglet Gérer les sources d'événements s'affiche.



3. Pour trier une colonne, cliquez sur + sur l'en-tête de cette colonne.

   Le menu déroulant Options de tri s'affiche.

4. Sélectionnez l'ordre de tri voulu.

Règles de surveillance

Utilisez la vue Politiques de surveillance pour gérer la configuration des alertes pour vos groupes de sources d'événement.

Vous pouvez créer des politiques qui émettent des alertes sur les groupes de sources d'événement en définissant des seuils et des notifications :

- Les seuils définissent des plages de fréquence des messages log. Vous pouvez spécifier un seuil bas, un seuil élevé ou les deux.
- Les notifications décrivent comment et où envoyer les alertes lorsque les seuils sont atteints.
- Pour créer des alertes basées sur la fréquence que vous spécifiez, vous utilisez une combinaison de seuils et de notifications.
- Si les alertes automatiques sont activées (c'est le cas par défaut), vous pouvez créer et activer une politique ***sans*** paramétrer de seuils. Si vous activez ensuite les notifications automatiques, les notifications seront envoyées lorsque la source d'événement dans le groupe se situe au-dessus ou au-dessous de son niveau de base pour la quantité spécifiée.

Par exemple, supposons que vous avez créé un groupe de sources d'événement composé de toutes les sources d'événement Windows basées au Royaume-Uni. Vous pouvez spécifier une politique qui vous avertit chaque fois qu'il se produit moins de 1 000 événements sur 30 minutes.

Remarque : En outre, ou au lieu de définir des règles de surveillance pour vos groupes de sources d'événement, vous pouvez Configuration des alertes automatiques pour afficher des alarmes lorsque le nombre de messages pour une source d'événement se situe en dehors des limites normales.

Configuration des alertes de groupes de sources d'événements

Chaque groupe de sources d'événements peut posséder sa propre règle d'alerte. Il est ainsi possible de paramétrer les limites de déclenchement d'alertes et le type de notification à utiliser en cas d'alerte. Cette rubrique décrit la procédure à suivre pour créer une règle d'alerte pour un groupe de sources d'événements.

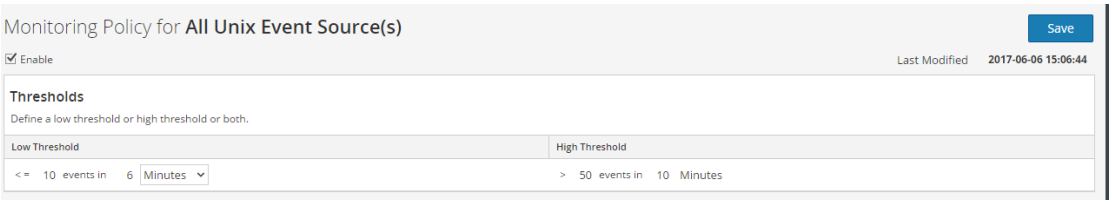
Procédures

Créer une règle d'alerte pour un groupe de sources d'événements

1. Accédez à **Administrateur > Sources d'événements**.
2. Sélectionnez l'onglet **Politiques de surveillance**.

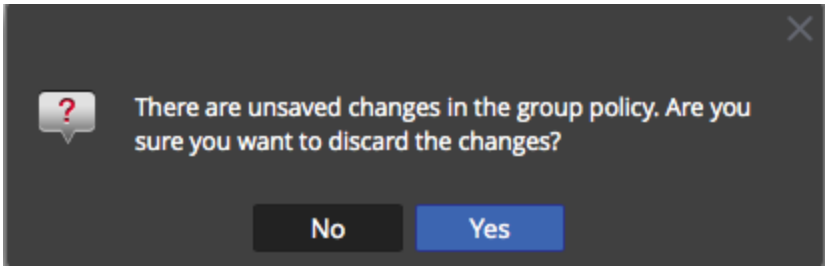
3. Dans le panneau **Groupes d'événement**, sélectionnez un groupe.
4. Saisissez une valeur dans les champs Seuil bas et Seuil élevé.

   Voici un exemple de seuils d'alerte.



5. Sélectionnez **Activer**, puis cliquez sur **Enregistrer** pour activer la règle d'alerte configurée.

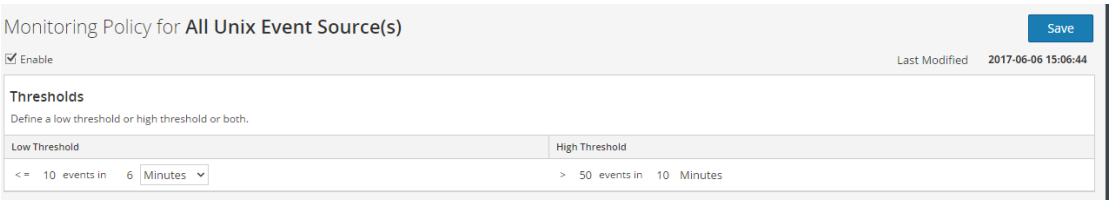
Remarque : Si vous modifiez une règle et quittez la page avant d'enregistrer vos modifications, un message d'avertissement vous indique que des modifications n'ont pas été enregistrées :



Définir et afficher les seuils d'une règle d'alerte

Chaque groupe de sources d'événements est également une politique d'alerte. Les seuils font partie d'une politique d'alerte. Vous pouvez définir des seuils pour chaque politique d'alerte. Pour chaque politique, vous pouvez définir un seuil bas, un seuil élevé ou les deux. En outre, vous pouvez activer une politique sans fixer de seuils. Cela vous permet de recevoir des notifications basées sur les alertes automatiques. Les alertes automatiques sont générées lorsque la valeur de base d'une source de l'événement se trouve en dehors des limites normales.

1. Accédez à **Administrateur > Sources d'événements**.
2. Sélectionnez l'onglet **Politiques de surveillance**.
3. Dans le panneau **Groupes d'événement**, sélectionnez un groupe.
   Les seuils définis pour le groupe sélectionné s'affichent dans le panneau **Seuils**.



4. Modifiez les valeurs pour le seuil bas ou haut comme suit :

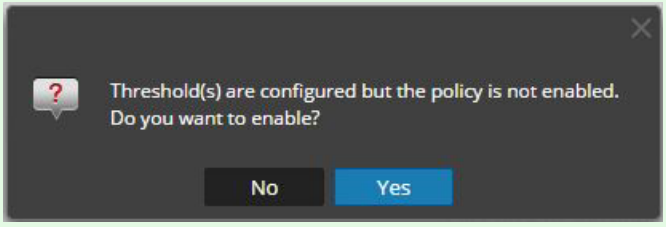
a. Saisissez le nombre d'événements pour le seuil.

b. Saisissez le nombre de minutes ou d'heures pour le seuil. La valeur minimale est de 5 minutes.

Remarque : Pour chaque seuil, vous pouvez définir les valeurs basses, les valeurs hautes ou les deux.

5. Sélectionnez **Activer** pour activer les alarmes lorsque les seuils ne sont pas atteints.

Remarque : Si vous configurez un seuil et si vous tentez d'enregistrer la page sans l'activer, vous recevez un message de confirmation vous demandant si la politique doit être activée :



Par exemple, supposons que vous saisissiez 10 et 30 comme valeurs pour le seuil bas : `10 events in 30 minutes`et 20 et 30 pour les valeurs du seuil élevé : `20 events in 30 minutes`. Cela signifie qu'entre 10 et 20 événements doivent être consignés en 30 minutes (pour le groupe de sources d'événements sélectionné). Cela signifie que tout nombre entre les seuils bas et haut est considéré comme normal et ne déclenche pas d'alarme.

Remarque : Une fois que vous avez ajouté un seuil pour une politique, vous ne pouvez pas le supprimer. Vous pouvez désactiver la politique ou définir le seuil bas ou haut sur 0 événement en 5 minutes. Cinq minutes est la durée minimale pour un seuil.

Configuration des notifications

Cette rubrique décrit comment configurer des notifications pour des groupes de source d'événement. Des notifications sont envoyées lorsque les seuils ne sont pas respectés.

Les notifications vont de pair avec les seuils. Avant de configurer les notifications, vous devez configurer les Seuils d'un groupe de source d'événement.

Remarque : Après avoir configuré les seuils pour un groupe de sources d'événements, si vous ne définissez pas de notifications, les utilisateurs ne sont pas informés même si une alarme se déclenche. Toutefois, l'ensemble des alarmes est visible sous l'onglet Onglet Alarmes.

Conditions préalables

Avant de configurer des notifications pour un groupe de source d'événement, vous devez examiner les éléments de notification disponibles :

- **Serveurs de notification :** Il s'agit des serveurs pour lesquels vous souhaitez recevoir des notifications système. Pour plus d'informations, consultez la rubrique **Présentation des serveurs de notification** dans le *Guide de configuration système*.
- **Modèles de notification :** Il s'agit des modèles disponibles pour chaque type de notification. Pour la gestion de la source d'événements, des modèles par défaut sont fournis pour E-mail (SMTP), SNMP et Syslog. Vous pouvez utiliser ces modèles tels quels, ou les personnaliser si nécessaire. Pour plus d'informations, consultez la rubrique **Présentation des modèles** dans le *Guide de configuration système*.
- **Sortie de notification :** Les sorties contiennent des paramètres pour le type de notification. Par exemple, le type de notification par e-mail contient les adresses e-mail et l'objet de la notification. Pour plus d'informations, consultez la rubrique **Présentation des sorties de notification** dans le *Guide de configuration système*.

Ajouter des notifications pour un groupe de source d'événement

Pour ajouter des notifications pour un groupe de source d'événement :

1. Accédez à **Administrateur > Sources d'événements**.
2. Sélectionnez l'onglet **Politiques de surveillance**.
3. Dans le panneau **Groupes d'événement**, sélectionnez un groupe.

   Remarque : Vous devriez déjà avoir fixé un seuil pour le groupe. Si ce n'est pas le cas, consultez Définir et afficher les seuils d'une règle d'alerte pour fixer un seuil, puis revenez à cette procédure. Par ailleurs, si les alertes automatiques sont activées, vous n'avez pas besoin de définir de seuils pour une politique. Les alarmes automatiques génèrent des notifications sans qu'il soit nécessaire de définir des seuils.

4. Dans le panneau Notifications, cliquez sur  , puis dans le menu déroulant, sélectionnez le type de notification que vous souhaitez ajouter :
   - E-mail
   - SNMP
   - Syslog

   Remarque : Des modèles ESM (Surveillance des sources d'événements) par défaut sont fournis pour chaque type de notifications.

5. Saisissez les valeurs dans les champs Notification, Serveur de notification, puis Modèles.

a. Pour la notification, sélectionnez-la dans la liste, ou ajoutez un type de notification approprié dans **Notifications**, puis sélectionnez-le ici.

b. Pour le serveur, sélectionnez en un dans la liste, ou ajoutez un serveur approprié dans **Notifications**, puis sélectionnez-le ici.

c. Pour le modèle, sélectionnez un modèle disponible, ou créez un modèle approprié dans **Notifications**, puis sélectionnez-le ici.

Remarque : Si vous devez ajouter ou modifier l'un de ces éléments, cliquez sur **Paramètres de notification**. Une nouvelle fenêtre de navigateur s'ouvre sur la page **Administration > Système > Notifications globales**. Utilisez cette page pour afficher ou mettre à jour les éléments de notification disponibles.

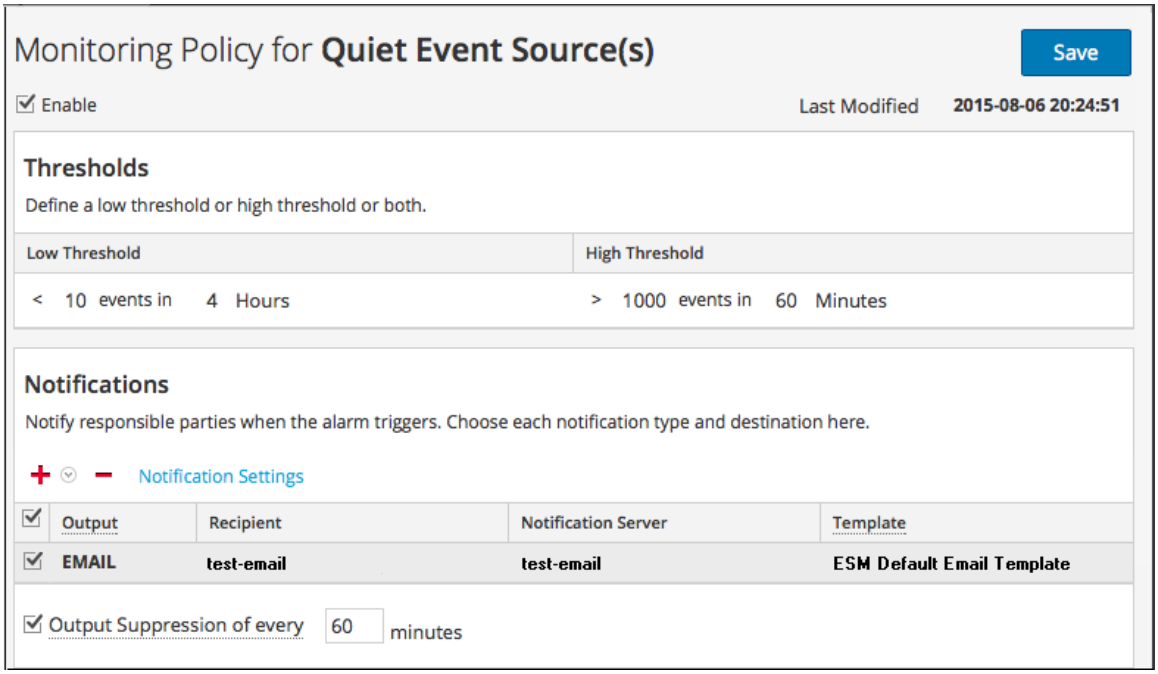
6. Vous pouvez également limiter le taux de notifications pour une politique.

a. Sélectionnez **Suppression de sortie** pour activer la définition d'une limite.

b. Saisissez une valeur, en minutes, pour le taux de suppression. Par exemple, si vous saisissez **30**, les notifications de cette politique sont limitées à une notification toutes les 30 minutes.

c. Cliquez sur **Enregistrer**.

Voici un exemple de règle de surveillance qui contient un seuil et une notification pour un groupe de source d'événement.



Désactivation des notifications

Des notifications sont envoyées lorsque des seuils ne sont pas respectés. En outre, des notifications automatiques sont envoyées lorsque les niveaux de base ne sont pas atteints. Cependant, vous pouvez déterminer que vous n'avez plus besoin de notifications pour les sources d'événement dans un groupe spécifique. Dans ce cas, vous pouvez désactiver les notifications pour le groupe de sources d'événement.

Remarque : Même si vous désactivez toutes les notifications, les détails des alarmes restent visibles dans l'Onglet Alarmes.

Conditions préalables

Vous devez avoir configuré les seuils et les notifications pour un groupe de sources d'événement et les avoir activés. Pour les notifications automatiques, vous devez sélectionner **Activer les notifications en mode Surveillance automatique** dans l'Onglet Alarmes.

Désactiver les notifications

Pour désactiver les notifications (manuelles et automatiques) pour un groupe de sources d'événement :

1. Accédez à **ADMIN > Sources d'événements**.
2. Sélectionnez l'onglet **Politiques de surveillance**.
3. Dans le panneau **Groupes d'événement**, sélectionnez un groupe.
4. Cliquez sur **Activer** pour supprimer la coche. Si vous désactivez cette option, les notifications ne sont pas envoyées pour ce groupe de sources d'événement même si les seuils ne sont pas respectés ou dépassés.
5. Vous pouvez aussi supprimer toutes les notifications. Toutefois, cette opération n'est pas nécessaire pour arrêter les notifications.

Affichage des alarmes des sources d'événements

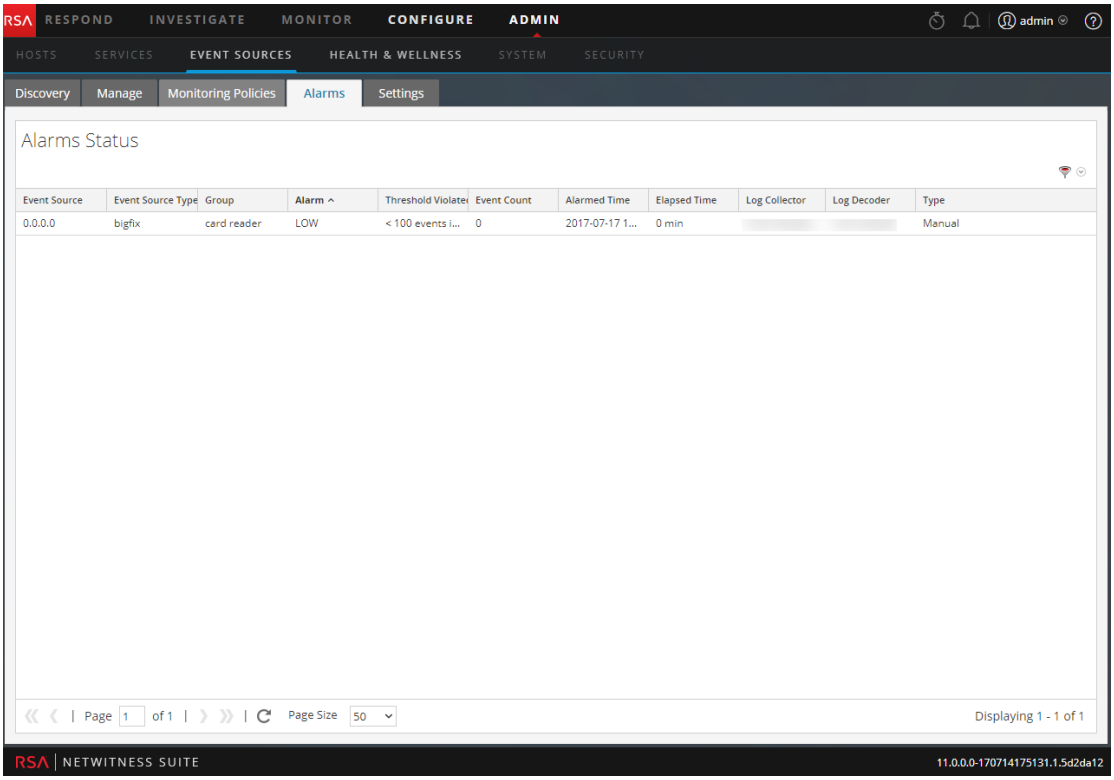
Cette rubrique décrit comment afficher les alarmes pour vos groupes de sources d'événements. Une fois que vous avez configuré et défini les alertes, vous pouvez afficher toutes les alarmes générées sous l'onglet **Alarmes** de la vue **Sources d'événements**.

Trier les informations liées aux alarmes

Lorsque vous accédez à cette vue pour la première fois, les données sont triées en fonction des alarmes les plus récentes (colonne Heure d'alarme). Vous pouvez effectuer un tri en fonction de n'importe quelle colonne.

1. Accédez à **ADMIN > Sources d'événements**.
2. Placez le pointeur de la souris sur la colonne que vous souhaitez trier.
3. Cliquez sur l'onglet **Alarmes**.
4. Placez le pointeur de la souris sur la colonne que vous souhaitez trier, puis cliquez sur l'icône .

   Voici un exemple de positionnement du pointeur de la souris sur la colonne Alarme.



5. Sélectionnez soit le **Tri croissant**, soit le **Tri décroissant** afin de trier la colonne de la

manière souhaitée.

Les données sont triées sur l'ensemble des pages.

Remarque : Vous pouvez également effectuer un tri sur deux colonnes. Pour cela, triez d'abord la deuxième colonne, puis triez la première colonne. Par exemple, si vous souhaitez afficher toutes les alarmes de niveau ÉLEVÉE en fonction de l'ordre des groupes, triez d'abord les **groupes**, puis triez les **alarmes**.

Filtrer les alarmes par type

Vous pouvez également filtrer les alarmes par type : vous pouvez afficher uniquement les alarmes (de base) manuelles ou automatiques. Pour effectuer un filtrage par type d'alarme, sélectionnez l'icône de filtre sur le côté droit de l'écran, dans la zone d'en-tête :

Sélectionnez Automatique ou Manuelle :

- Si vous sélectionnez Automatique, seules les alertes basées sur les lignes de base sont affichées.
- Si vous sélectionnez Manuelle, seules les alarmes pour lesquelles vous avez défini des seuils sont affichées.

Configuration des alertes automatiques

Remarque : Les alertes automatiques, et leurs paramètres, sont actuellement en phase de test bêta.

Conditions préalables

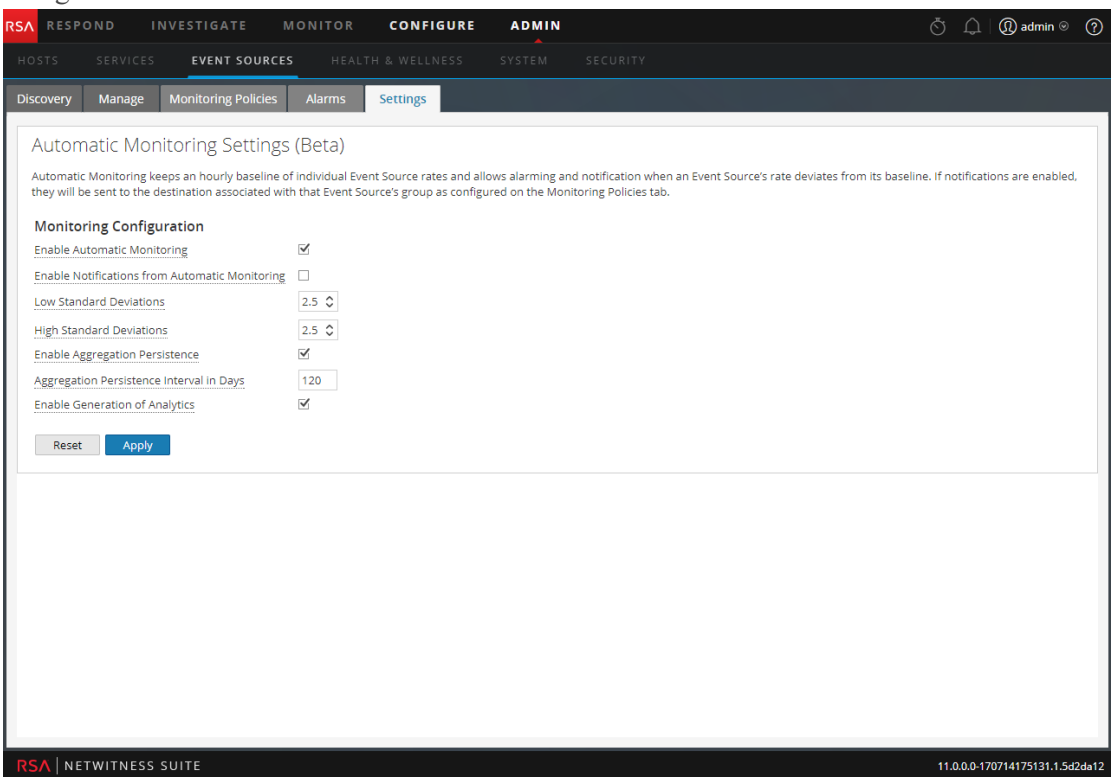
Avant de configurer des notifications pour un groupe de source d'événement, vous devez examiner les éléments de notification disponibles :

- **Serveurs de notification :** Il s'agit des serveurs pour lesquels vous souhaitez recevoir des notifications système. Pour plus d'informations, consultez la rubrique **Présentation des serveurs de notification** dans le *Guide de configuration système*.
- **Modèles de notification :** Il s'agit des modèles disponibles pour chaque type de notification. Pour la gestion de la source d'événements, des modèles par défaut sont fournis pour E-mail (SMTP), SNMP et Syslog. Vous pouvez utiliser ces modèles tels quels, ou les personnaliser si nécessaire. Pour plus d'informations, consultez la rubrique **Présentation des modèles** dans le *Guide de configuration système*.
- **Sortie de notification :** Les sorties contiennent des paramètres pour le type de notification. Par exemple, le type de notification par e-mail contient les adresses e-mail et l'objet de la notification. Pour plus d'informations, consultez la rubrique **Présentation des sorties de notification** dans le *Guide de configuration système*.

Pour configurer les alertes automatiques :

1. Accédez à **Administrateur > Sources d'événements**.
2. Sélectionnez l'onglet **Paramètres**.

L'onglet Paramètres s'affiche.



3. Par défaut, la surveillance automatique est activée. Pour désactiver les alertes automatiques, décochez l'option **Activer la surveillance automatique**.
4. Par défaut, les notifications pour les alertes automatiques sont désactivées. Pour activer les notifications automatiques, sélectionnez l'option **Activer les notifications en mode Surveillance automatique**.
5. Configurez les paramètres en fonction de vos modèles d'utilisation :
   - **Écarts types faibles** : écarts types au-dessous desquels vous souhaitez recevoir des alertes. La valeur par défaut est **2.0** (95 % de confiance).
   - **Écarts types élevés** : écarts types au-dessus desquels vous souhaitez recevoir des alertes. La valeur par défaut est **2.0** (95 % de confiance).

   Remarque : Vous pouvez ajuster les paramètres d'écart type standard par incréments de 0,1 (un dixième) de l'écart type standard.
6. Cliquez sur **Enregistrer** pour fermer la boîte de dialogue et enregistrer vos paramètres.

Résolution des problèmes de gestion de source d’événements

Rubriques de dépannage :

Problèmes liés aux alarmes et aux notifications

Cette rubrique décrit la façon d'aborder les problèmes que vous pouvez rencontrer avec les alarmes ou les notifications.

Alarmes

Si vous ne voyez pas les alarmes prévues, vérifiez que vous avez configuré tous les éléments nécessaires, comme indiqué ci-dessous.

Alarmes automatiques

Pour voir les alarmes automatiques sur l'écran Alarmes, vous devez sélectionner l'option **Activer la surveillance automatique**.

Cette option se trouve sous l'onglet **Paramètres** (**Administrateur** > **Sources d'événements** > **Paramètres**) et est sélectionnée par défaut. Cependant, il se peut qu'une autre personne ait désactivé l'option.

Alarmes manuelles

Pour voir les alarmes manuelles sur l'écran Alarmes, toutes les conditions suivantes doivent être réunies :

- La source de l'événement doit faire partie d'un groupe.
- Un seuil inférieur ou supérieur (ou les deux) doit être défini dans le cadre d'une politique de groupe.
- La politique de groupe doit être activée.

Notifications

Si vous voyez des alarmes, mais que vous ne recevez pas les notifications prévues, vérifiez que vous avez configuré tous les éléments nécessaires, comme indiqué ci-dessous.

Vérifiez également que vous avez correctement configuré les serveurs de notification et les sorties de notification. Vous effectuez une grande partie de la configuration préliminaire des notifications via **Administrateur > Système > Notifications globales**. Pour plus d'informations, consultez la rubrique **Panneau Notifications globales** dans le*Guide de Configuration système*.

Notifications automatiques

Pour que le système envoie des notifications automatiques, toutes les conditions suivantes doivent être réunies :

- L'option **Activer la surveillance automatique** doit être sélectionnée (cette option est sélectionnée par défaut).
- L'option **Activer les notifications en mode Surveillance automatique** doit être sélectionnée. Cette option est désactivée par défaut. Par conséquent, vous (ou une autre personne de l'organisation) devez la sélectionner. Pour voir cette option, accédez à **Administrateur** > **Sources d'événements** > **Paramètres**.
- La source de l'événement qui a déclenché l'alarme doit faire partie d'un groupe pour lequel une politique est activée. Notez qu'il n'est pas nécessaire de définir des seuils pour les notifications automatiques.
- Au moins une notification doit être configurée pour la politique (e-mail, SNMP ou Syslog).

Notifications manuelles

Pour que le système envoie des notifications manuelles (c'est-à-dire des notifications qui indiquent qu'une alarme manuelle a été déclenchée) :

- La source de l'événement qui a déclenché l'alarme doit faire partie d'un groupe pour lequel une politique de groupe est activée.
- Un seuil doit être défini pour la politique.
- Au moins une notification doit être configurée pour la politique.

Messages de log en double

Il est possible de collecter des messages depuis la même source d'événement sur deux Log Collectors ou plus. Cette rubrique décrit ce problème et les moyens de le résoudre.

Détails

Si l'agrégateur ESM détecte les mêmes événements pour la même source d'événement sur différents Log Collectors, vous recevez un avertissement similaire au texte suivant :

```
2015-03-17 15:25:29,221 [pool-1-thread-6] WARN
com.rsa.smc.esm.groups.events.listeners.EsmStatEventListener -
 192.0.2.21-apache had a previous event only 0 seconds ago; likely
because it exists on multiple log collectors
```

Ce message d'avertissement signifie que la source d'événement `192.0.2.22-apache` est collectée par plusieurs hôtes. Vous pouvez visualiser la liste des hôtes dans la colonne Log Collector dans l'onglet **Gérer** de la fenêtre Administration > Vue Sources d'événements.

Effacez les messages en double.

1. Arrêtez collectd sur NetWitness Suite et les Log Decoders :

   ```
   Service collectd stop
   ```

2. Supprimez le fichier ESM Aggregator conservé sur NetWitness Suite :

   ```
   rm /var/lib/netwitness/collectd/ESMAggregator
   ```

3. Réinitialisez le Log Decoder.

   a. Accédez au Log Decoder REST, à l'adresse `http://<LD_IP_Address>:50102`.

   b. Cliquez sur **decoder(*)** pour afficher les propriétés du Decoder.

   c. Dans le menu déroulant Propriétés, sélectionnez **Réinitialiser** et cliquez sur **Envoyer**.

4. Dans le panneau Sources d'événement de l'onglet Gérer des sources d'événement,

   sélectionnez toutes les sources d'événement et cliquez sur − pour les supprimer.

Résoudre les problèmes liés aux feeds

L'objectif du générateur de flux est de générer le mappage d'une source d'événement sur la liste de groupes auxquels elle appartient.

Si vous disposez d'une source d'événement à partir de laquelle vous collectez des messages qui ne figure pas encore dans les groupes de sources d'événement appropriés, cette rubrique fournit des références et des informations générales pour vous aider à traquer le problème.

Détails

Le feed ESM mappe plusieurs clés sur une valeur unique. Il mappe les attributs DeviceAddress, Forwarder et DeviceType à groupName.

Le but du feed ESM est d'enrichir la méta de l'événement source avec le groupName collecté sur Log Decoder.

Fonctionnement

Le générateur de feed est prévu pour se mettre à jour chaque minute. Cependant, il ne se déclenche qu'en cas de changements (créer, mettre à jour ou supprimer) dans les sources ou les groupes d'événements.

Il génère un fichier de feed unique avec une source d'événement au mappage de groupe, et envoie le même feed sur tous les Log Decoder qui sont connectés à NetWitness Suite.

Une fois le fichier de feed chargé sur les Log Decoder, pour tous les nouveaux événements, il enrichit les métadonnées des événements avec groupName, et ajoute ce groupName à logstats.

Une fois que groupName se trouve dans logstats, ESM Aggregator groupe les informations et les envoie à ESM. À ce stade, vous devriez voir la colonne **Nom du groupe** sous l'onglet **Surveillance des sources d'événements**.

L'ensemble du processus peut prendre un certain temps. Par conséquent, vous devrez peut-être attendre plusieurs secondes après avoir ajouté une nouvelle source de groupe ou d'événement, avant que le nom du groupe ne s'affiche.

Remarque : Si l'attribut du type de source de l'événement change lorsque le feed est mis à jour, NetWitness Suite ajoute une nouvelle entrée logstats, plutôt que de mettre à jour l'entrée existante. Ainsi, il y a deux entrées de logstats différentes dans logdecoder. Auparavant, les messages existants auraient été répertoriés dans le type précédent. Tous les nouveaux messages sont enregistrés pour le nouveau type de source d'événement.

Fichier de feed

Le format du fichier de feed est le suivant :

`DeviceAddress, Forwarder, DeviceType, GroupName`

`DeviceAddress` est soit `ipv4, ipv6`, soit `hostname`, selon ce qui a été défini pour la source d'événement.

Voici un exemple de fichier de feed :

```
"12.12.12.12","d6","NETFLOW","grp1"
"12.12.12.12","ld4","netflow","grp1"
"12.12.12.12","d6","netfow","grp1"
"0:E:507:E6:D4DB:E:59C:A","10.25.50.243","apache","Apac
hegrp"
"1.2.3.4","LCC","apache","Apachegrp"
"10.100.33.234","LC1","apache","Apachegrp"
"10.25.50.248","10.25.50.242","apache","Apachegrp"
"10.25.50.251","10.25.50.241","apache","Apachegrp"
"10.25.50.252","10.25.50.255","apache","Apachegrp"
```

```
"10.25.50.253","10.25.50.251","apache","Apachegrp"
"10.25.50.254","10.25.50.230","apache","Apachegrp"
"10.25.50.255","10.25.50.254","apache","Apachegrp"
"13.13.13.13","LC1","apache","Apachegrp"
"AB:F255:9:8:6C88:EEC:44CE:7",,"apache","Apachegrp"
"Appliance1234",,"apache","Apachegrp"
"CB:F255:9:8:6C88:EEC:44CE:7","10.25.50.253","apache","
Apachegrp"
```

Résoudre les problèmes liés aux feeds

Vous pouvez vérifier les éléments suivants pour vérifier où le problème se produit.

Log Decoders 10.5

Vos NetWitness Suite Log Decoders ont-ils la version 10.5 ou supérieure ? Si ce n'est pas le cas, vous devez les mettre à niveau. Pour la version NetWitness Suite 10.6, les feeds ne sont envoyés qu'à la version Log Decoder 10.5 et supérieure.

Existence des fichiers de feed

Vérifiez que l'archive ZIP contenant les feeds existe à l'emplacement suivant :

`/opt/rsa/sms/esmfeed.zip`

Ne modifiez pas ce fichier.

Groupe méta rempli sur LD

Vérifiez que le groupe méta est rempli sur Log Decoder. Naviguez vers le REST de Log Decoder et vérifiez logstats :

`http://LogDecoderIP:50102/decoder?msg=logStats&force-content-type=text/plain`

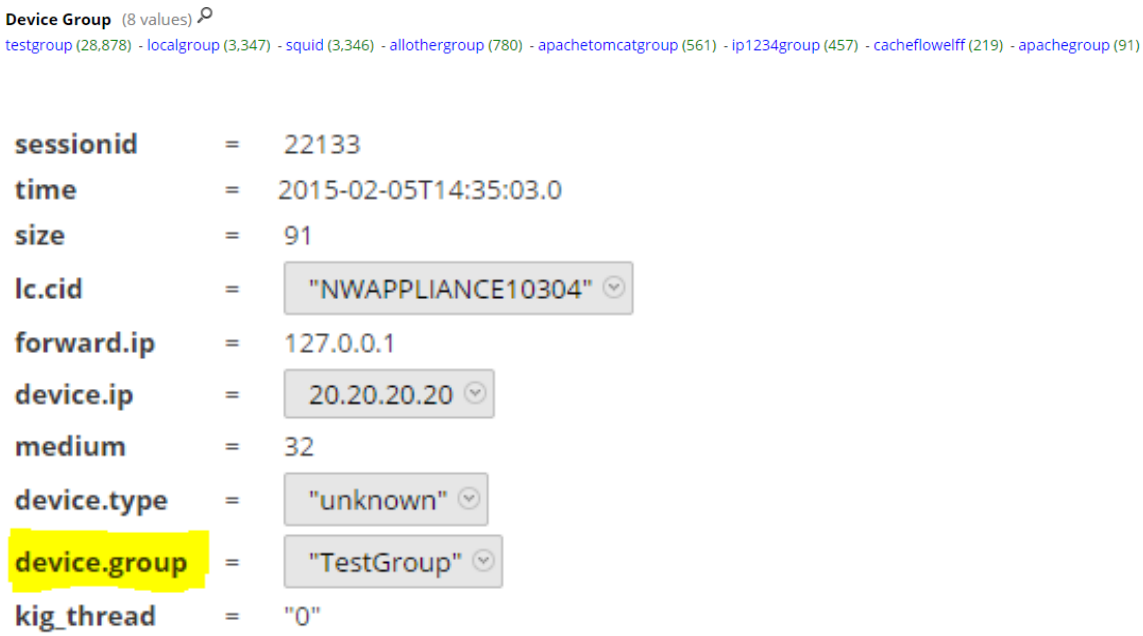
Voici un exemple de fichier logstats avec des informations de groupe :

```
device=apache forwarder=NWAPPLIANCE10304 source=1.2.3.4
count=338 lastSeenTime=2015-Feb-04 22:30:19
lastUpdatedTime=2015-Feb-04 22:30:19
groups=IP1234Group,apacheGroup
device=apachetomcat forwarder=NWAPPLIANCE10304
source=5.6.7.8 count=1301 lastSeenTime=2015-Feb-04
22:30:19 lastUpdatedTime=2015-Feb-04 22:30:19
groups=AllOtherGroup,ApacheTomcatGroup
```

Dans le texte ci-dessus, les informations du groupe sont en gras.

Méta du groupe de périphériques sur Concentrator

Vérifiez que la méta du **Groupe de périphériques** existe sur le Concentrator et que les événements comportent des valeurs dans le champ `device.group`.



Fichier log SMS

Vérifiez le fichier log SMS à l'emplacement suivant pour afficher les messages d'information et d'erreur : `/opt/rsa/sms/logs/sms.log`

Voici des exemples de messages *d'information* :

```
Feed generator triggered...
Created CSV feed file.
Created zip feed file.
Pushed ESM Feed to LogDeocder : <logdecoder IP>
```

Voici des exemples de messages *d'erreur* :

```
 Error creating CSV File : <reason>Unable to push the
ESM Feed: Unable to create feed zip archive.
Failed to add Group in CSV: GroupName: <groupName> :
Error: <error>
Unable to push the ESM Feed: CSV file is empty, make
sure you have al-least on group with al-least one
eventsource.
Unable to push the ESM Feed: No LogDecoders found.
Unable to push the ESM Feed: Unable to push feed file
```

```
on LogDecoder-<logdecoderIP>Unable to push the ESM
Feed: admin@<logdecoderIP>:50002/decoder/parsers
received error: The zip archive
"/etc/netwitness/ng/upload/<esmfeedfileName>.zip" could
not be opened
Unable to push the ESM Feed: <reason>
```

Vérifiez que les données Logstats sont lues et publiées par ESMReader et ESMAggregator

Voici les étapes de vérification de collecte des logstats par **collectd** et de leur publication dans la gestion de source d'événements.

ESMReader

1. Sur les Log Decoders, ajoutez la balise **debug "true"** dans**/etc/collectd.d/NwLogDecoder_ESM.conf** :

```
#
# Copyright (c) 2014 RSA The Security Division of EMC
#
<Plugin generic_cpp>    PluginModulePath "/usr/lib64/collectd"
    debug "true"

    <Module "NgEsmReader" "all">
        port      "56002"
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-
6737-4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7-   ba7e9a165aae.pem"
        interval  "600"
        query     "all"
        <stats>
        </stats>
    </Module>
    <Module "NgEsmReader" "update">
        port      "56002"
        ssl       "yes"
        keypath   "/var/lib/puppet/ssl/private_keys/d4c6dcd4-
6737-4838-a2f7-    ba7e9a165aae.pem"
        certpath  "/var/lib/puppet/ssl/certs/d4c6dcd4-6737-4838-
a2f7-   ba7e9a165aae.pem"
        interval  "60"
        query     "update"
        <stats>
```

```
            </stats>
        </Module>
    </Plugin>
```

2. Exécutez la commande :

   ```
   collectd service restart
   ```

3. Exécutez la commande suivante :

   ```
   tail –f /var/log/messages | grep collectd
   ```

   Vérifiez que ESMReader lit logstats et qu'il n'y a pas d'erreur. S'il existe des problèmes de lecture, vous verrez des erreurs similaires à ce qui suit :

   ```
   Apr 29 18:47:45 NWAPPLIANCE15788 collectd[14569]: DEBUG: NgEsmReader_
   all: error getting ESM data for field "groups" from logstat
   device=checkpointfw1 forwarder=PSRTEST source=1.11.51.212. Reason:
   <reason>Apr 29 18:58:36 NWAPPLIANCE15788 collectd[14569]: DEBUG:
   NgEsmReader_update: error getting ESM data for field "forwarder" from
   logstat device=apachetomcat source=10.31.204.240. Reason: <reason>
   ```

ESMAggregator

1. Dans NetWitness Suite, supprimez les commentaires de la balise verbose dans **/etc/collectd.d/ESMAggregator.conf** :

   ```
   # ESMAggregator module collectd.conf configuration file
   #
   # Copyright (c) 2014 RSA The Security Divsion of EMC
   #
   <Plugin generic_cpp>
   PluginModulePath "/usr/lib64/collectd"
   <Module "ESMAggregator">
           verbose 1
           interval "60"
           cache_save_interval "600"
           persistence_dir "/var/lib/netwitness/collectd"
   </Module>
   </Plugin>
   ```

2. Exécutez ce qui suit :

   ```
   collectd service restart.
   ```

3. Exécutez la commande suivante :

   ```
   run "tail –f /var/log/messages | grep ESMA
   ```

Recherchez les données ESMAggregator et assurez-vous que votre entrée logstat est disponible dans les logs.

Exemple de sortie :

```
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = d4c6dcd4-6737-4838-a2f7-ba7e9a165aae
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174451
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
Dispatching ESM stat NWAPPLIANCE15788/esma_update-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
decoders
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[0] logdecoder[0] = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[1] logdecoder_utcLastUpdate[0] = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[2] groups = Cacheflowelff,Mixed
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[3] logdecoders = 767354a8-5e84-4317-bc6a-52e4f4d8bfff
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
MetaData[4] utcLastUpdate = 1425174470
Mar  1 02:32:08 NWAPPLIANCE15936 collectd[11203]: ESMAggregator:
Dispatching RRD stat NWAPPLIANCE15788/esma_rrd-cacheflowelff/esm_
counter-3.3.3.3 with a value of 1752 for
NWAPPLIANCE15788/cacheflowelff/esm_counter-3.3.3.3 aggregated from 1 log
```

Configurer l'intervalle de tâche du générateur de feed JMX

Bien que la tâche de génération de feed est prévue pour s'exécuter chaque minute par défaut, vous pouvez la modifier avec **jconsole**, le cas échéant.

Pour modifier l'intervalle de tâche du générateur de flux :

1. Ouvrez **jconsole** pour le service SMS.
2. Sous l'onglet MBeans, accédez à **com.rsa.netwitness.sms** > **API** > **esmConfiguration** > **Attributs**.
3. Modifiez la valeur de la propriété **FeedGeneratorJobIntervalInMinutes**.
4. Accédez à **Opérations** sous la même arborescence de navigation, puis cliquez sur **commit ()**. Cette opération enregistre la nouvelle valeur dans le fichier JSON correspondant sous **/opt/rsa/sms/conf** et utilise la valeur si SMS est redémarré.

La définition d'une nouvelle valeur replanifie la tâche du générateur de flux pour le nouvel intervalle.

Problèmes liés à l'importation de fichiers

Si votre fichier d'importation n'est pas mis en forme correctement, ou s'il manque des informations requises, un message d'erreur s'affiche et le fichier n'est pas importé.

Vérifiez les éléments suivants :

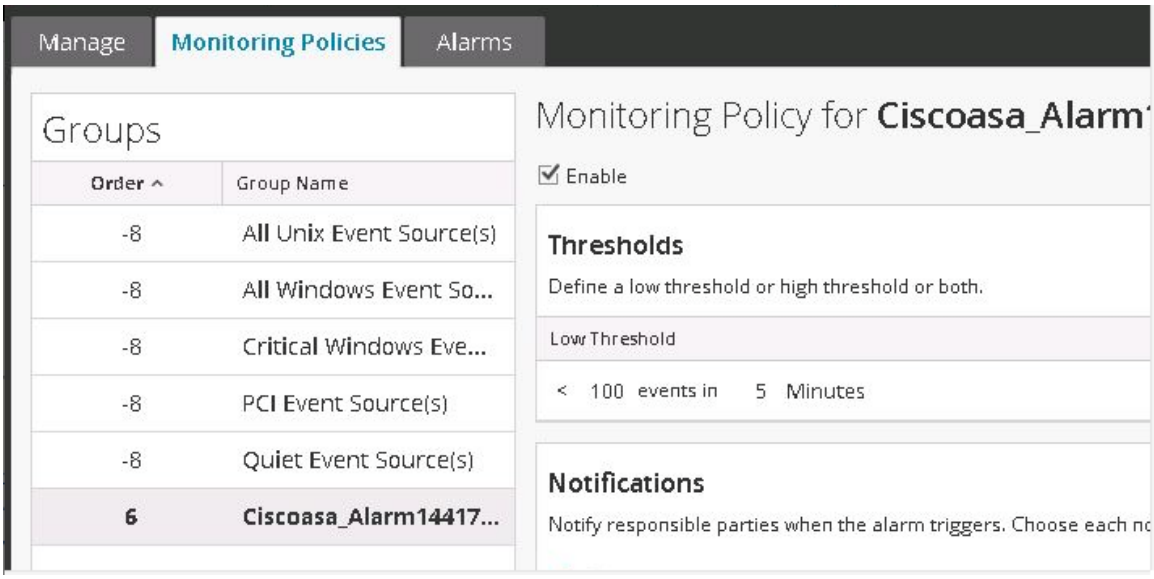
- Si vous ajoutez des sources inconnues, chaque ligne du fichier devra contenir une combinaison des attributs requis :
  - IP ou IPv6 ou Nom d'hôte et
  - Type de source d'événement
- La première ligne du fichier doit contenir les noms des en-têtes qui doivent correspondre aux noms présents dans NetWitness Suite. Pour obtenir la liste des noms de colonnes corrects, vous pouvez exporter une seule source d'événement. Examinez le fichier CSV exporté : la première ligne du fichier contient l'ensemble des noms d'attributs/de colonnes appropriés.

Valeurs négatives dans les politiques

Des valeurs négatives peuvent apparaître dans le champ Classer de la section Groupes, dans l'onglet Politiques de surveillance. Cette rubrique décrit une solution de contournement pour restaurer la numérotation correcte dans vos politiques.

Détails

L'écran suivant montre un exemple de situation où le nombre des politiques de groupes devient négatif.



Si vous rencontrez cette situation, glissez-déplacez le groupe du haut (**Toutes les sources d'événement Unix** dans l'image ci-dessus) après le dernier groupe (**Ciscoasa_Alarm14417**). Cela restaure la numérotation normale (ordinale). Vous pouvez alors continuer à glisser-déplacer les groupes jusqu'à ce qu'ils soient dans un ordre adapté à votre organisation.

Effacez les messages en double.

1. Arrêtez collectd sur NetWitness Suite et les Log Decoders :

   ```
   Service collectd stop
   ```

2. Supprimez le fichier ESM Aggregator conservé sur NetWitness Suite :

   ```
   rm /var/lib/netwitness/collectd/ESMAggregator
   ```

3. Réinitialisez le Log Decoder.

   a. Accédez au Log Decoder REST, à l'adresse `http://<LD_IP_Address>:50102`

   b. Cliquez sur **decoder(*)** pour afficher les propriétés du Decoder.

   c. Dans le menu déroulant Propriétés, sélectionnez **Réinitialiser** et cliquez sur **Envoyer**.

4. Dans le panneau Sources d'événement de l'onglet Gérer des sources d'événement,

   sélectionnez toutes les sources d'événement et cliquez sur − pour les supprimer.

Référence à Event Source Management

Rubriques de référence à ESM :

Onglet Alarmes

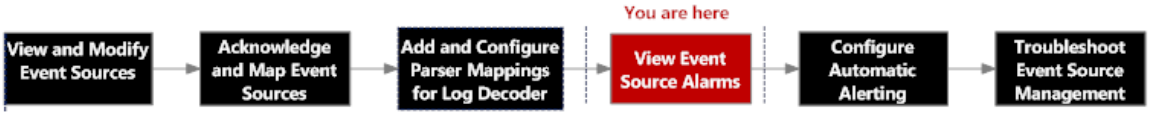
Sous l'onglet Alarmes, vous pouvez afficher les détails des alarmes qui ont été générées.

L'onglet Alarmes comporte un panneau qui affiche l'état de l'alarme.

Pour accéder à cet onglet, accédez à ADMIN > Sources d'événements > Alarmes.

Workflow

Ce workflow montre l'ensemble du processus de configuration des sources d'événements. Il indique également l'emplacement dans le processus de la configuration des paramètres d'alarmes et d'alertes.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Définir un seuil d'alarme.	Gestion des groupes de sources d'événements
Administrateur	Modifier les paramètres de seuil d'alarme.	Gestion des groupes de sources d'événements

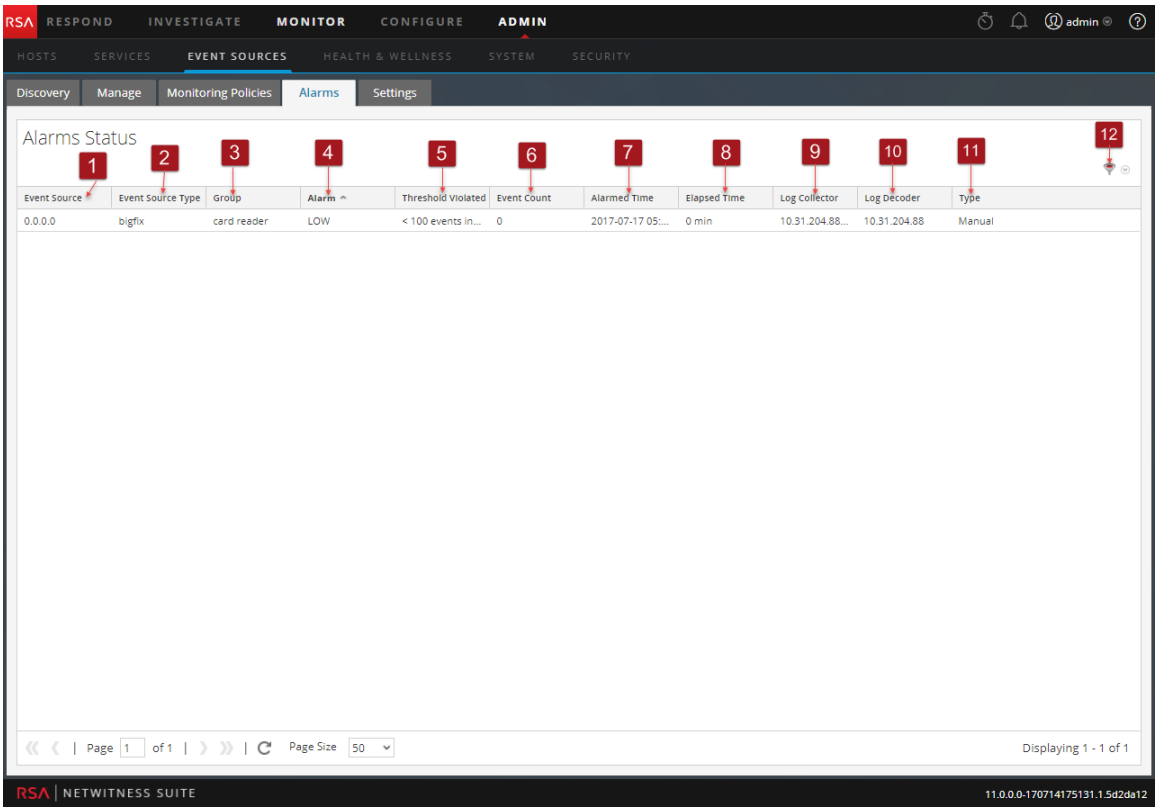
Rubriques connexes

Affichage des alarmes des sources d'événements

Gestion des groupes de sources d'événements

Aperçu rapide

L'onglet Alarmes présente le détail des sources d'événements qui enfreignent une règle et un seuil. Seules les sources d'événements qui enfreignent une règle apparaissent dans la liste. Une fois que la source de l'événement revient à un état normal, l'alarme correspondante disparaît de la liste.

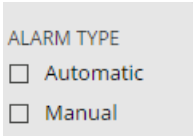


1	IP, IPv6 ou Nom d'hôte de la source d'événement à l'état d'alarme.
2	Type de la source de l'événement à l'état d'alarme. Exemple : **winevent_nic** (pour Microsoft Windows) ou **rhlinux** (pour Linux).
3	Affiche le groupe de sources d'événements qui contient la source de l'événement pour laquelle l'alarme a été déclenchée.
4	Affiche le type de seuil déclenché : **Élevé** ou **Bas**
5	Affiche les conditions du seuil déclenché. Par exemple : `5,000,000 events in 5 minutes`
6	Affiche le nombre d'événements durant la période de seuil déclenchant l'alarme.
7	Affiche l'heure initiale à laquelle la source de l'événement est passée à l'état d'alarme. **Remarque :** Lorsque vous accédez à cette vue pour la première fois, les données sont triées en fonction de cette colonne (l'alarme la plus récente apparaissant en premier).
8	Affiche le temps écoulé depuis que la source de l'événement est passée à l'état d'alarme.
9	Affiche la dernière collecte extraite de cette source d'événement par le Log Collector.
10	Affiche la dernière réception de cette source d'événement par Log Decoder.

11 Affiche le type d'alarmes. Le type d'alarmes est **Manuelle** ou **Automatique** :

- **Manuelle** : il s'agit des alarmes qui enfreignent la règle de seuil configurée.
- **Automatique** : il s'agit des alarmes qui dévient de la base de référence pour la source d'événement à l'état d'alarme.

12 Sélectionnez l'icône **Filtrer** pour afficher le menu **Filtrer** :



Sélectionnez **Automatique** ou **Manuelle** :

- Si vous sélectionnez **Automatique**, seules les alertes basées sur les bases de référence sont affichées.
- Si vous sélectionnez **Manuelle**, seules les alarmes pour lesquelles vous avez défini des seuils sont affichées.

Remarque : Vous pouvez masquer ou afficher des colonnes. Pour ce faire, cliquez avec le bouton droit de la souris dans le titre du tableau, puis choisissez **Colonnes** dans le menu déroulant. Sélectionnez une colonne pour l'afficher, ou désactivezła pour la masquer.

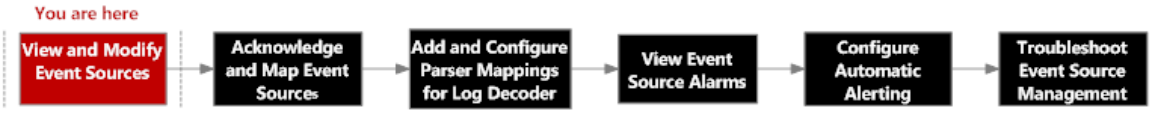
Onglet Découverte

Pour accéder à cet onglet, cliquez sur NetWitness ADMIN> Sources d'événements. L'onglet Découverte s'affiche.

L'onglet Découverte vous permet d'examiner les types de sources d'événements que NetWitness a découvert pour chaque adresse et le degré de précision avec lequel le système les a identifiés. Si les types de sources d'événements découverts sont corrects, vous pouvez accepter de filtrer cette source d'événement. S'ils sont incorrects, vous pouvez définir les types de sources d'événements autorisés pour une adresse spécifique afin que les futurs logs puissent être analysés par rapport aux parsers corrects.

Workflow

Ce workflow montre l'ensemble du processus de configuration des sources d'événements.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Reconnaître que les types de sources d'événements découverts sont corrects.	Reconnaissance et mappage des sources d'événements
Administrateur	Mapper les analyseurs qui doivent être utilisés pour une source d'événement lorsque les types découverts ne sont pas tout à fait exacts.	Reconnaissance et mappage des sources d'événements

Rubriques connexes

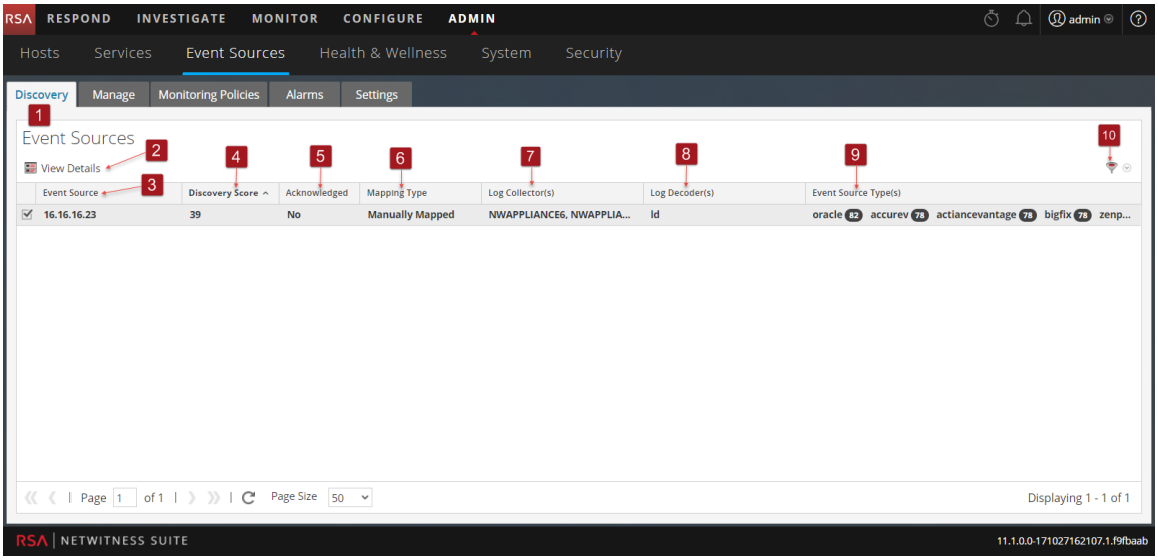
Gérer les mappages d'analyseurs

Vue Détails

Aperçu rapide

L'exemple suivant affiche une liste d'adresses et les types de sources d'événements découverts. Les types de sources d'événements affichent les sources d'événements qui ont été découvertes.

Voici un exemple de l'onglet.



1	Affiche le panneau Source d'événement avec l'onglet Découverte ouvert.
2	Affiche le bouton Détails, qui permet de consulter les détails de la source d'événement sélectionnée.
3	Affiche l'adresse de la source d'événement sélectionnée.
4	Affiche le score de découverte de la source d'événement sélectionnée.
5	Affiche si la source d'événement sélectionnée a été reconnue ou non.
6	Affiche le type de mappage de la source d'événement sélectionnée : Automatique, Mappé manuellement ou Aucun. Les modifications apportées au mappage ne sont affichées qu'ici.
7	Affiche les noms d'hôte des Log Collectors qui contiennent les sources d'événements.
8	Affiche les noms d'hôte des Log Decoders qui contiennent les sources d'événements.
9	Affiche les types de sources d'événements découverts et leurs scores de découverte associés.
10	Affiche les filtres Afficher la confirmation et Afficher le mappage avec les options permettant de découvrir et de mapper les sources d'événements sélectionnées.

Barre d'outils et fonctions

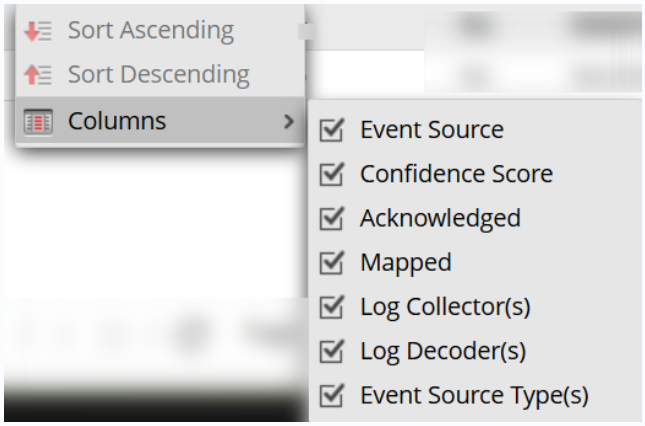
L'onglet Découverte contient les fonctions suivantes :

Champ	Description
Outils 	L'élément suivant est disponible dans la barre d'outils : **Afficher les détails** : Fournit des détails sur la source d'événement sélectionnée.
Source d'événement	IP, IPv6 ou nom d'hôte de la source d'événement
Score de découverte	Affiche la note globale de découverte associée à cette adresse spécifique. Les scores élevés indiquent une meilleure fiabilité. Les scores de découverte ont une valeur allant de 0 (score le moins sûr) à 100 (score le plus sûr).
Confirmé	Les sélections sont **Oui** (vous avez reconnu la source d'événement) ou **Non** (vous n'avez pas reconnu la source d'événement).
Mappé	Les sélections sont **Oui** (vous avez mappé la source d'événement) ou **Non** (vous n'avez pas mappé la source d'événement).
Services Log Collector	Services Log Collector ayant reçu des logs à partir de cette adresse de source d'événement.
Services Log Decoder	Services Log Decoder ayant reçu des logs à partir de cette adresse de source d'événement.
Types de sources d'événements	Types d'adresses de sources d'événements analysés et score de découverte correspondant pour chaque type.

Remarque : Les scores de découverte ne sont disponibles que pour les services Log Decoder 11.0.0.0 et versions ultérieures. Les scores de découverte pour les versions de Log Decoder antérieures à 11.0.0.0 s'affichent comme étant indisponibles.

Le tableau suivant décrit l'ordre de tri des scores de découverte. Pour accéder au menu déroulant Ordre de tri, cliquez sur la flèche vers le bas de la colonne Sources d'événements.

Champ	Description
Tri croissant	Trie la colonne par son score de découverte dans l'ordre croissant.

Champ	Description
Tri décroissant	Trie la colonne par son score de découverte dans l'ordre décroissant.
Colonnes	Utilisé pour masquer ou afficher une ou plusieurs colonnes, comme illustré dans l'exemple suivant. 

Vue Détails

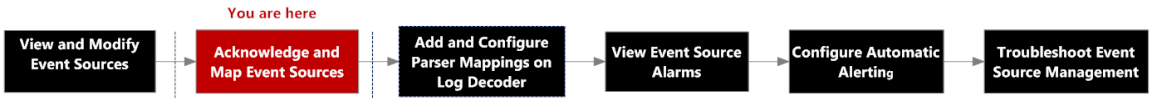
La vue **Détails** permet d'afficher des détails sur la source d'événement, ainsi qu'un échantillon des logs identifiés pour chaque type afin de vérifier leur exactitude.

Vous pouvez accéder à la vue **Détails** de plusieurs façons.

- Dans la barre d'outils, cliquez sur le bouton **Afficher les détails**. Vous pouvez également
- Double-cliquer sur la source d'événement que vous avez sélectionnée.

Workflow

Ce workflow montre l'ensemble du processus de configuration des sources d'événements.



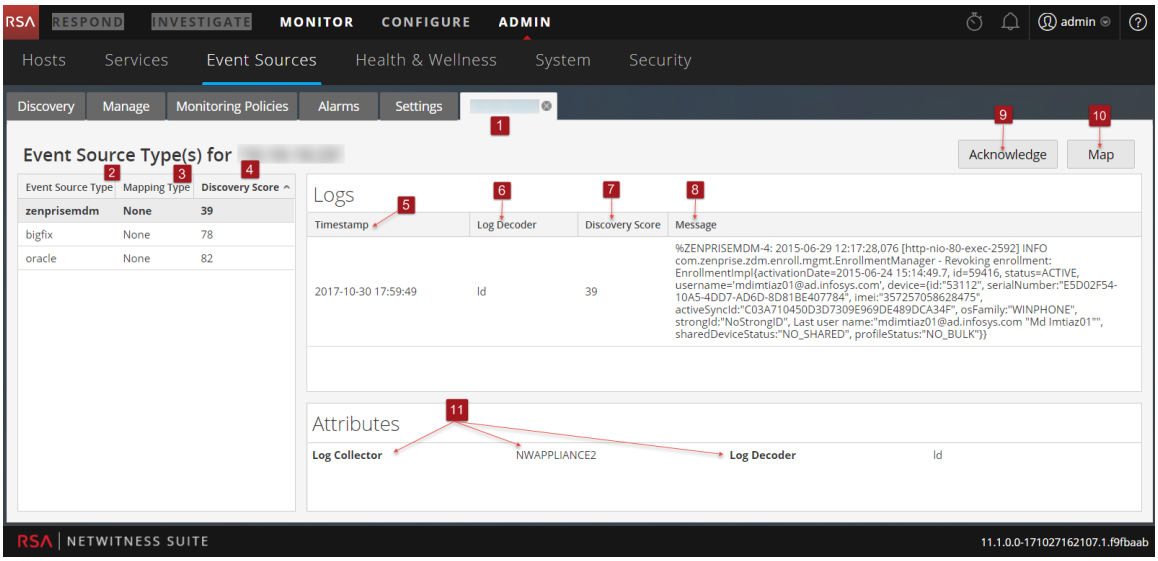
Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Afficher les logs pour un Log Decoder version 10.6.	Affichage des logs à partir des versions de Log Decoder antérieures à 11.0.0.0
Administrateur	Reconnaître que tous les types de sources d'événements découverts sont corrects.	Gérer les mappages d'analyseurs
Administrateur	Mapper les sources d'événements sélectionnées.	Gérer les mappages d'analyseurs

Aperçu rapide

L'exemple suivant présente les scores de découverte, les types de sources d'événements, les logs et les attributs qui correspondent à la source d'événement que vous avez sélectionnée dans le panneau Sources d'événements pour un seul Log Decoder.

Remarque : Les logs de périphériques ne sont disponibles que pour les versions de Log Decoder 11.0.0.0 et ultérieures.



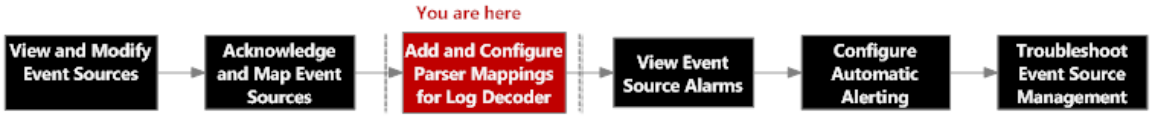
1	Affiche l'adresse de la source d'événement sélectionnée.
2	Affiche le type de la source d'événement sélectionnée.
3	Affiche le type de mappage de la source d'événement sélectionnée : Automatique, Mappé manuellement ou Aucun. Les modifications apportées au mappage de la source d'événement ne sont affichées qu'ici.
4	Affiche le score de découverte de la source d'événement sélectionnée, de la moins sûre (0) à la plus sûre (100).
5	Affiche les horodatages des derniers logs analysés en fonction du type de source d'événement sélectionné.
6	Affiche l'adresse du Log Decoder qui analyse les sources d'événements.
7	Affiche le score de découverte du log correspondant.
8	Affiche les logs du type de source d'événement sélectionné.
9	Vous permet de reconnaître que tous les types de sources d'événements découverts sont corrects.
10	Vous permet de définir les analyseurs appropriés pour les adresses de sources d'événements sélectionnées.
11	Affiche les attributs de gestion des sources d'événements pour le type de source d'événement sélectionné.

Gérer les mappages d'analyseurs

La boîte de dialogue **Gérer les mappages d'analyseurs** vous permet de mapper les analyseurs appropriés pour des adresses de sources d'événements sélectionnées. À partir de la vue **Détails**, sélectionnez le bouton **Mapper**.

Workflow

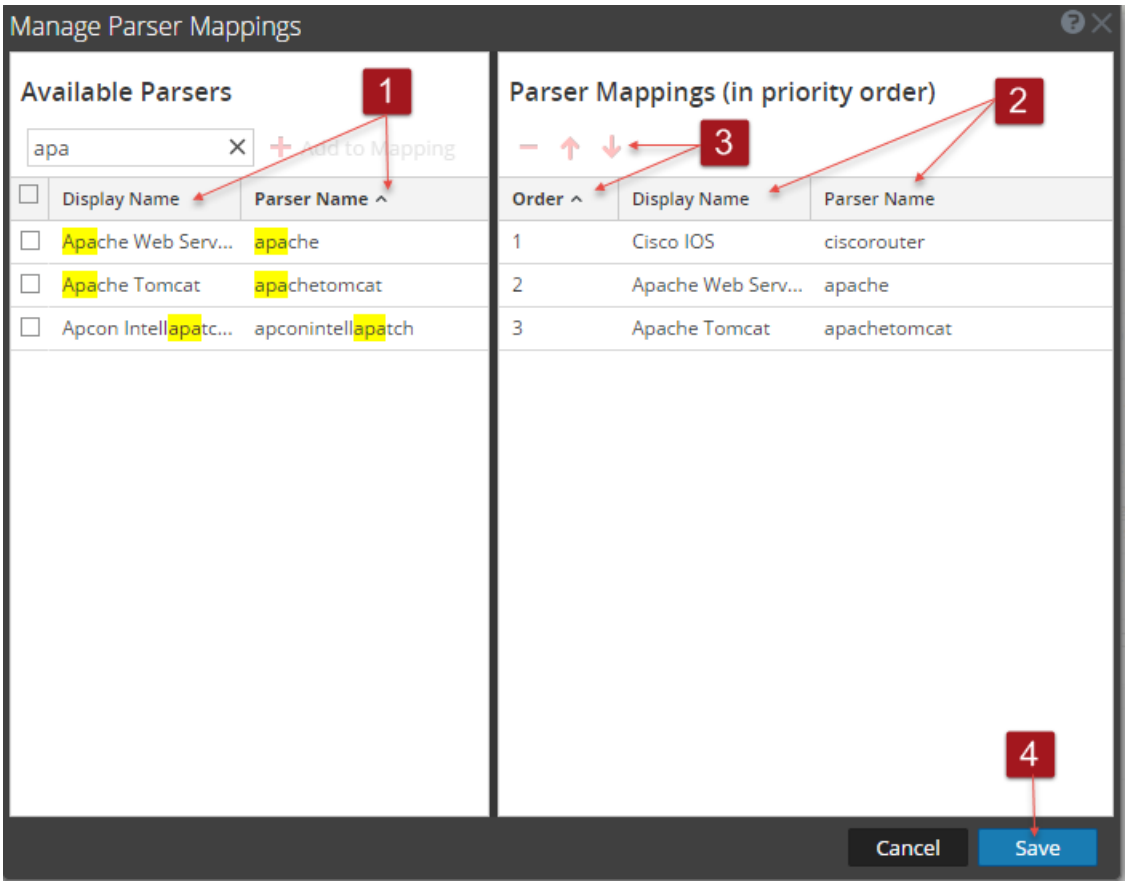
Ce workflow montre l'ensemble du processus de configuration des sources d'événements.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Mapper les analyseurs pour les adresses de sources d'événements sélectionnées.	Vue Détails

Aperçu rapide



1	Affiche tous les analyseurs disponibles que vous pouvez mapper en fonction des sources d'événements que vous avez sélectionnées dans la vue **Découverte**. Affiche également les mappages déjà présents dans les Log Decoders pour la source d'événement sélectionnée ou les analyseurs qui ont été découverts. Pour filtrer vos analyseurs disponibles, saisissez les premières lettres du nom de l'analyseur que vous souhaitez mapper. Cliquez sur le bouton **Ajouter au mappage** pour ajouter l'analyseur aux mappages d'analyseurs répertoriés dans le panneau de droite. Vous devez sélectionner des analyseurs avant de cliquer sur le bouton **Ajouter aumappage**. Ajoutez l'analyseur sélectionné en cliquant sur le bouton **Ajouter au mappage** dans le panneau de droite. Vous pouvez réorganiser les mappages d'analyseurs à l'aide des touches fléchées vers le haut ⬆ et vers le bas ⬇ et vous pouvez également glisser-déplacer les mappages d'analyseurs sélectionnés. Vous pouvez sélectionner plusieurs mappages en appuyant sur la touche **Ctrl**.
2	Affiche les noms des analyseurs sélectionnés que vous souhaitez mapper.
3	Affiche l'ordre des mappages d'analyseurs sélectionnés.

Vous pouvez supprimer des mappages d'analyseurs en sélectionnant le signe moins ( ).
Appuyez sur la touche **Ctrl** pour sélectionner plusieurs mappages afin d'effectuer des opérations de groupe sur ces derniers.

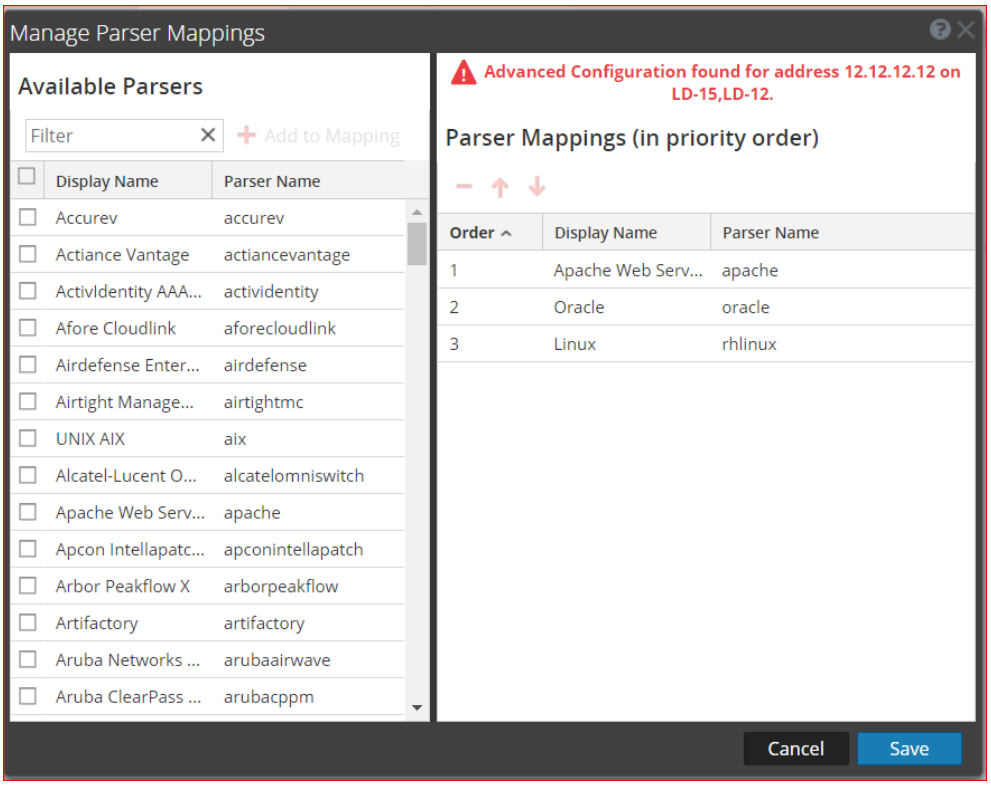
4 Cliquez sur **Enregistrer** pour enregistrer vos mappages pour tous les Log Decoders. Un message vous informe que les mappages sont correctement enregistrés. Lorsque la fenêtre est fermée, la bannière de l'onglet **Détails** est mise à jour pour refléter l'état. S'il est mappé, le texte affiché est **Mappé**.
Cliquez sur **Annuler** pour revenir à l'onglet **Détails**.

Configuration avancée

Les configurations de mappages avec le Log Collector ne sont pas affichées dans la fenêtre Mappages d'analyseurs. Si le mappage est enregistré, il est enregistré pour l'adresse IP correspondante, pas pour l'entrée Log Collector correspondante. Si aucun mappage n'est trouvé pour l'adresse IP correspondante, les types de sources d'événements découverts s'affichent dans la fenêtre Mappages d'analyseur.

Si des configurations Log Decoder avancées sont découvertes, un message similaire à celui ci-dessous s'affiche dans la boîte de dialogue Gérer les mappages d'analyseurs.

Remarque : Si vous souhaitez modifier la configuration avancée, vous devez accéder à la configuration de mappages d'analyseurs du service Log Decoder.

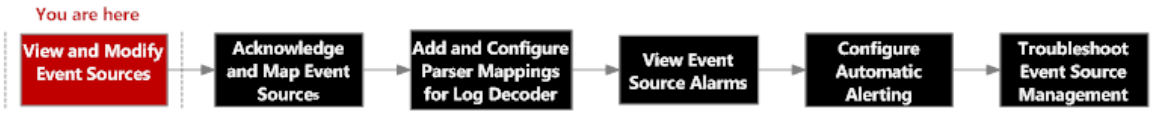


Créer/modifier un formulaire de groupe

Le formulaire Créer des groupes de sources d'événements s'affiche lorsque vous créez ou modifiez un groupe de sources d'événements.

Workflow

Ce workflow montre l'ensemble du processus de configuration des sources d'événements.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Créer ou modifier un groupe de source d'événement.	Formulaire de création de groupes de sources d'événements Création de groupes de sources d'événements Modification ou suppression des groupes de sources d'événements
Administrateur	Gérer des groupes de sources d'événements.	Gestion des groupes de sources d'événements

Rubriques connexes

Formulaire de création de groupes de sources d'événements

Gestion des groupes de sources d'événements

Vue Sources d'événements

Le panneau Attributs de source d'événement propose les onglets suivants.

Pour accéder à ce panneau, accédez à **ADMIN> Sources d'événements**.

Workflow

Ce workflow montre le processus complet pour la modification, la reconnaissance, le mappage et la configuration des sources d'événements, ainsi que l'affichage et la configuration des alertes et des alarmes des sources d'événements.

Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Créer un groupe de source d'événement.	Création de groupes de sources d'événements
Administrateur	Modifier ou supprimer un groupe de sources d'événements.	Modification ou suppression des groupes de sources d'événements
Administrateur	Modifier les attributs d'une source d'événement	Création d'une source d'événement et modification des attributs

Rubriques connexes

Gestion des groupes de sources d'événements

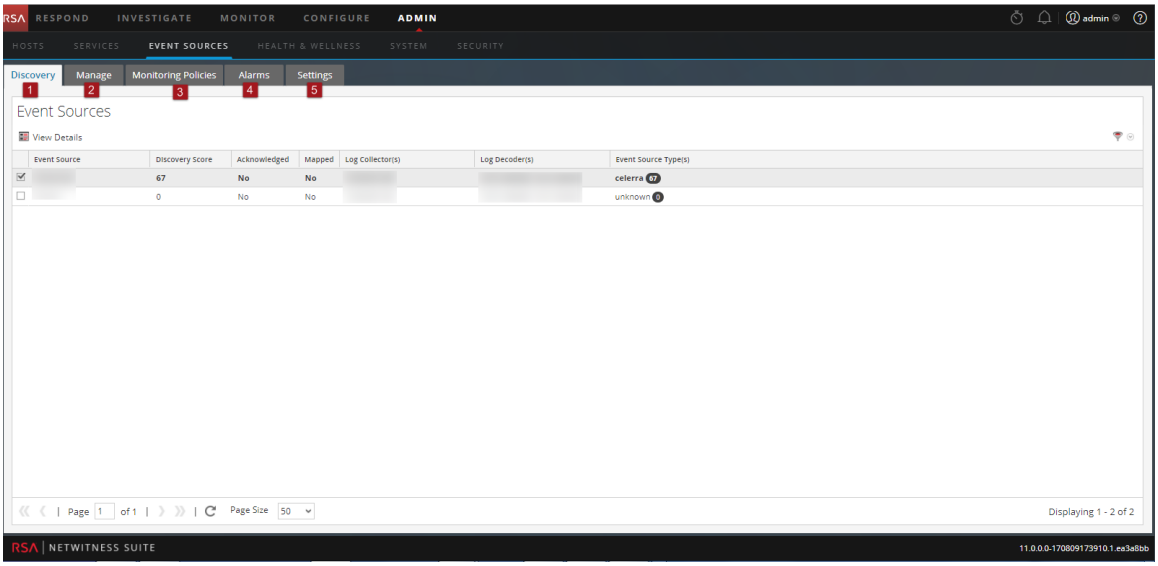
Création de groupes de sources d'événements

Modification ou suppression des groupes de sources d'événements

Création d'une source d'événement et modification des attributs

Aperçu rapide

La vue Sources d'événements présente les détails des Sources d'événements qui sont découverts, reconnus ou mappés par NetWitness.



1	Onglet Découverte Utilisez cet onglet pour consulter les types de sources d'événements que NetWitness a découvert pour chaque adresse et le degré de précision avec lequel le système les a identifiés.
2	Onglet Gérer Utilisez cet onglet pour créer, modifier et supprimer des groupes de sources d'événements. Il présente une vue personnalisable permettant d'effectuer des recherches sur toutes les sources et tous les groupes d'événements.
3	Onglet Règles de surveillance Utilisez cet onglet pour gérer la configuration des alertes des sources d'événements.
4	Onglet Alarmes Utilisez cet onglet pour afficher les détails des alarmes générées.
5	Onglet Paramètres Utilisez cet onglet pour afficher ou modifier le comportement des alertes automatiques (de base).

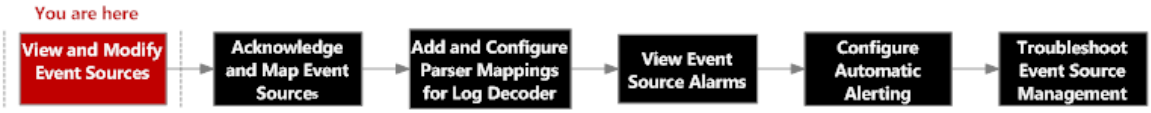
Onglet Gérer

L'onglet Gérer permet d'organiser les sources d'événements en groupes, et affiche les attributs pour chaque source d'événement.

Pour accéder à cet onglet, accédez à **ADMIN > Sources d'événements**.
L'onglet **Gérer** s'affiche par défaut.

Workflow

Ce workflow montre l'ensemble du processus de configuration des sources d'événements.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Créer un groupe de source d'événement.	Création de groupes de sources d'événements
Administrateur	Modifier ou supprimer un groupe de sources d'événements.	Gestion des groupes de sources d'événements

Rubriques connexes

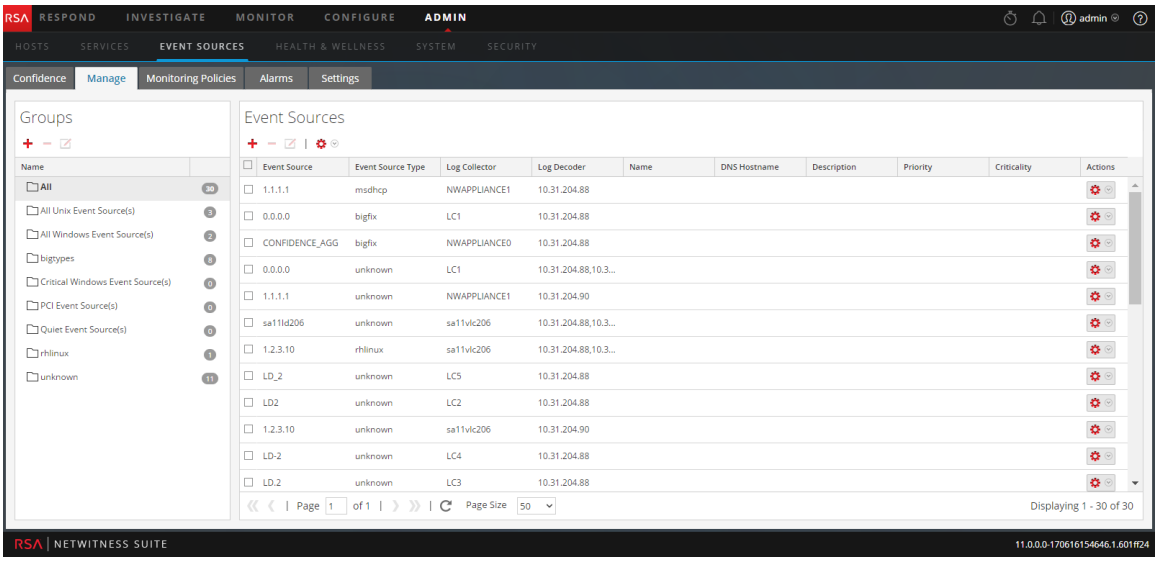
Création de groupes de sources d'événements

Gestion des groupes de sources d'événements

Création d'une source d'événement et modification des attributs

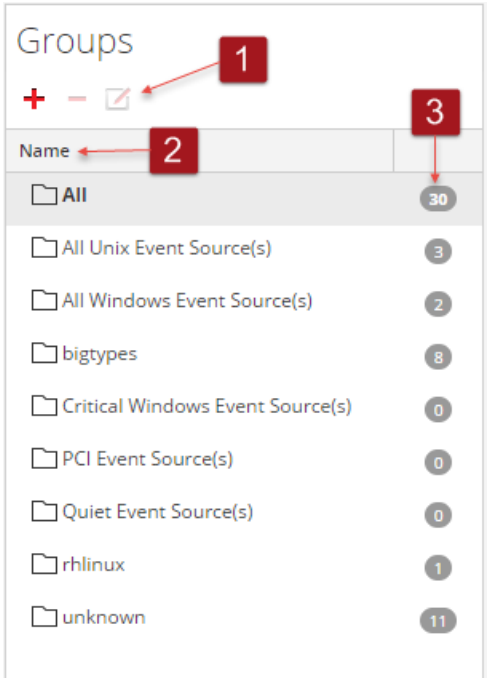
Aperçu rapide

L'onglet Gérer permet d'organiser les sources d'événements en groupes, et affiche les attributs pour chaque source d'événement. L'onglet Gérer comporte deux panneaux, Groupes et Sources d'événements.



Panneau Groupes

Le panneau Groupes affiche les groupes de sources d'événements, ainsi que le nombre de membres pour chaque groupe. Pour afficher toutes les sources d'événements, sélectionnez **Tout** dans la liste des groupes. Voici un exemple du panneau Groupes.



1	Affiche les icônes standard de NetWitness Suite permettant d'ajouter, de supprimer ou de modifier des groupes.
2	Indique l'identifiant de chaque groupe dans la colonne Nom. Vous pouvez utiliser les noms des groupes pour identifier rapidement les critères utilisés pour constituer le groupe.

Par exemple, si vous créez un groupe composé de sources d'événements Windows pour l'organisation Sales, vous pourriez nommer le groupe **Sources Windows Sales**.

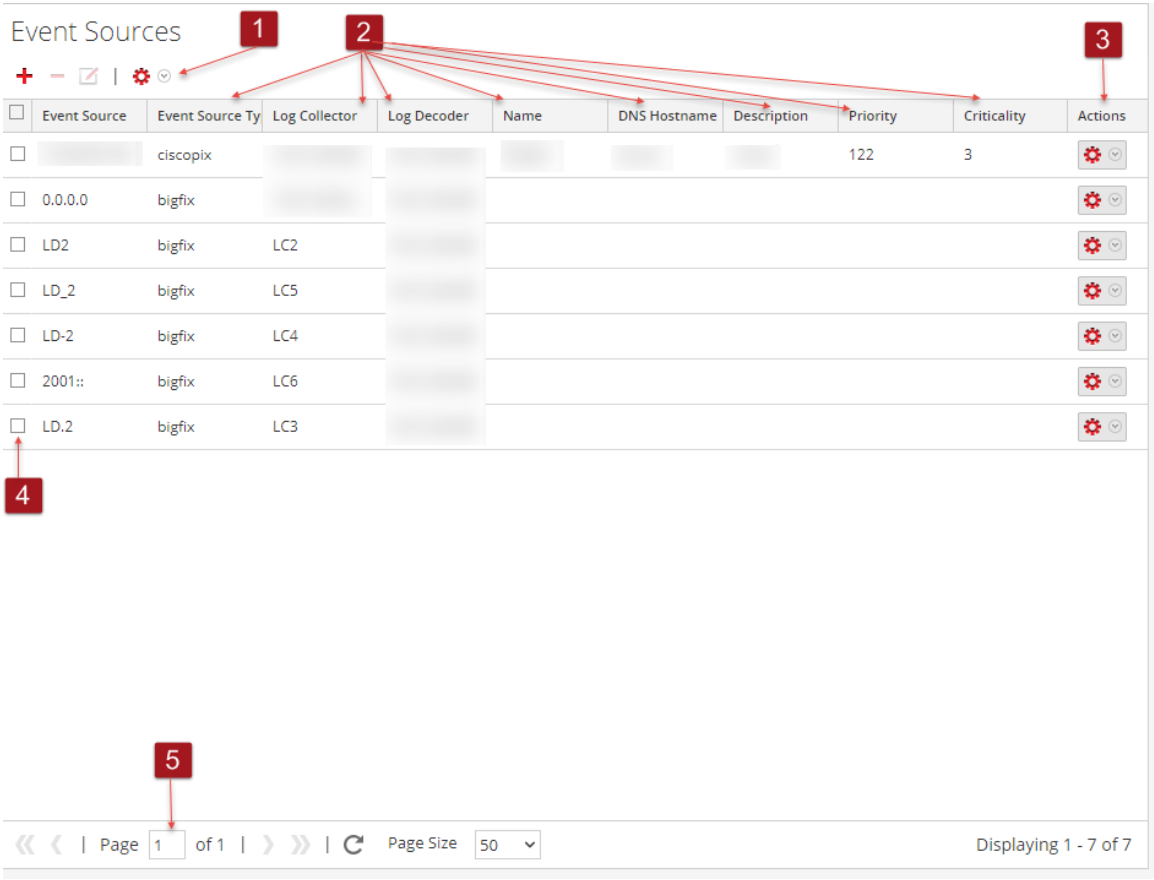
Remarque : Le nom du groupe de sources d'événements n'est pas modifiable. Une fois que vous avez créé un groupe, ce nom existe aussi longtemps que le groupe lui-même.

3 Indique le nombre de sources d'événements contenues dans un groupe. Autrement dit, le nombre de sources d'événements correspondant aux critères permettant de définir le groupe.

Remarque : Le nombre n'est pas mis à jour de manière dynamique lorsque de nouvelles sources d'événements sont ajoutées. Donc, vous devrez actualiser l'affichage pour mettre à jour le nombre de groupes affiché.

Panneau Sources d'événements

Le panneau Sources d'événements affiche les attributs des sources d'événements dans le groupe sélectionné. Ou si l'option Tout est sélectionnée dans le panneau Groupes, le panneau Sources d'événements affichera toutes les sources d'événements.



1	La barre d'outils inclut les outils suivants :
	• **Ajouter** : ajoute manuellement une source d'événement
	• **Supprimer** : supprime une source d'événement
	• **Edit** : met à jour les attributs d'une source d'événement existante
	• Menu **Importer/Exporter** : affiche un menu avec les options suivantes :
	  • **Importer** : importe les sources d'événements CMDB (Content Management Database), d'une feuille de calcul ou d'un autre outil.
	  • **Exporter** : exporte les sources d'événements sélectionnées et leurs attributs au format CSV.
	  • **Exporter le groupe** : exporte le groupe entier qui est actuellement sélectionné.

2	Affichage en colonnes des attributs. Vous pouvez choisir les attributs à afficher.
3	Actions: Menu contextuel pour les commandes fréquemment utilisées : modifier, supprimer et exporter
4	Cases à cocher : Sélectionnez les lignes à utiliser lors de l'exécution de tâches sur plusieurs sources d'événements, comme la modification en bloc.
5	Outils de navigation : Au bas de l'écran figurent des options qui vous permettent de naviguer dans votre groupe : • **Page *x* sur *y*** : indique quelle page est affichée actuellement et le nombre de pages total existant pour ce groupe. • <<, <, > et >> : cliquez sur ces icônes pour vous déplacer entre les pages, une à la fois (< et >) ou la première (<<) ou dernière (>>) page. • **Taille de la page** : utilisez ce sélecteur pour choisir la taille de votre page. • **Affichage *x* - *y* sur *z*** : vérification rapide des sources d'événement actuellement affichées sur le nombre total pour le groupe.

Tri

Dans le panneau Sources d'événements, la liste des options est présentée dans un ordre trié. Vous pouvez choisir la colonne sur laquelle trier. Notez toutefois que l'ordre de tri dépend des majuscules .

Pour les colonnes de chaînes, si les valeurs contiennent un mélange de lettres minuscules et de lettres majuscules, ces dernières s'afficheront en tête de liste avant les valeurs en lettres minuscules.

Par exemple, imaginons que la colonne Type de source d'événement contienne les entrées suivantes : Netflow, APACHE, netwitnesspectrum, ciscoasa L'ordre de tri serait le suivant :

- APACHE
- Netflow
- ciscoasa
- netwitnessspectrum

Onglet Gérer la source d'événement

L'écran Gérer la source d'événement contient plusieurs composants intégrés qui présentent différentes perspectives d'une source d'événement.

- Afficher les détails de la source d'événement
- Ajouter des valeurs d'attribut à une source d'événement
- Supprimer des valeurs d'attribut pour une source d'événement

Pour afficher l'écran Gérer la source d'événement pour une source d'événement :

1. Accédez à **ADMIN > Sources d'événements**.
2. Sélectionnez l'onglet **Gérer**.
3. Dans le volet Sources d'événements, sélectionnez une source d'événement dans la liste et cliquez sur +.

Workflow

Ce workflow montre le processus complet pour la modification, la reconnaissance, le mappage et la configuration des sources d'événements, ainsi que l'affichage et la configuration des alertes et des alarmes des sources d'événements.

Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Créer un groupe de sources d'événements qui contient toutes les sources d'événements haute priorité.	Création de groupes de sources d'événements
Administrateur	Modifier les attributs d'une source d'événement	Création d'une source d'événement et modification des attributs

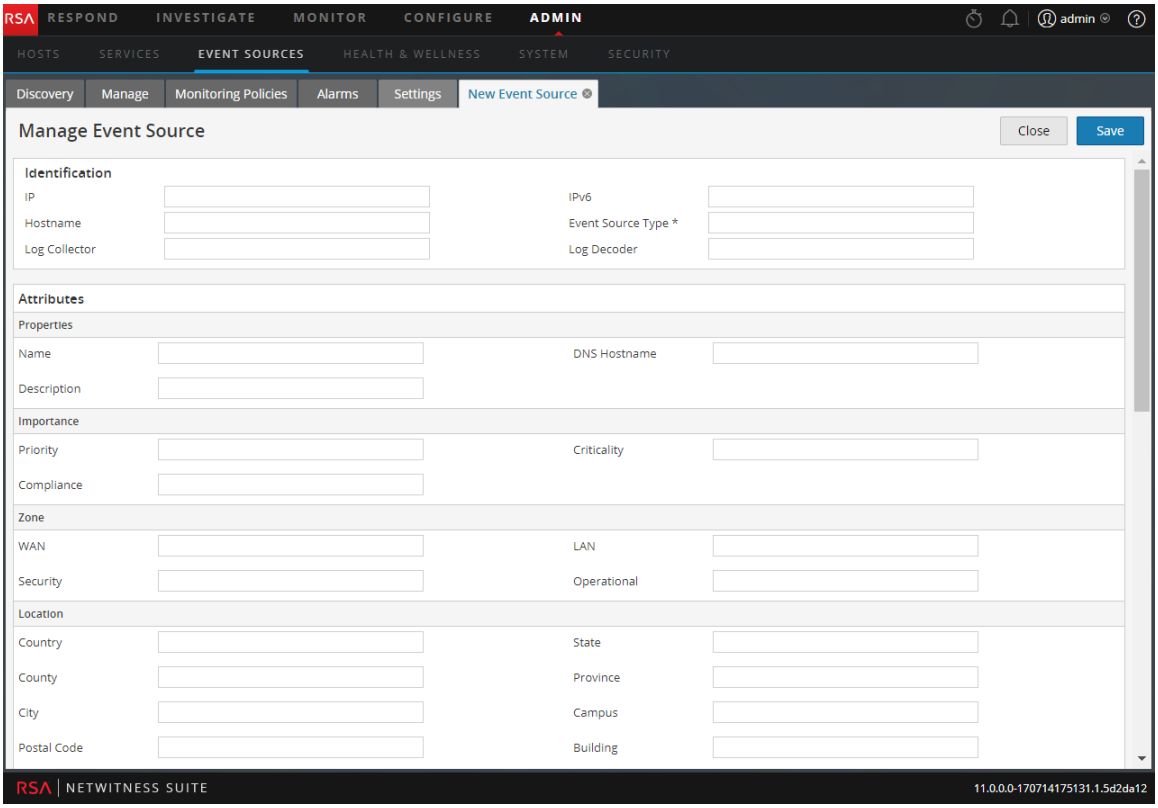
Rubriques connexes

Création d'une source d'événement et modification des attributs

Création de groupes de sources d'événements

Aperçu rapide

Voici un exemple de l'onglet Nouvelle source d'événement :



Ce tableau décrit les catégories d'attributs des sources d'événements.

Section d'attribut	Description
Identification	Ces attributs sont les principaux attributs qui identifient collectivement une source d'événement. Les attributs suivants sont remplis automatiquement et ne peuvent pas être modifiés sur cet écran : • Adresse IP • Valeur IPv6 • Nom de l'hôte • Type de source d'événement Ces attributs peuvent être modifiés : • Log Collector • Log Decoder
Propriétés	Ces attributs fournissent le nom et la description. • Nom • Nom d'hôte DNS • Description
Importance	Ces attributs peuvent être utilisés pour le regroupement par priorité. • Priorité • Degré de criticité • Compliance
Zone	Ces attributs peuvent être utilisés pour le regroupement par zone. • WAN (Wide Area Network) • LAN (Local Area Network) • Sécurité • Operational

Section d'attribut	Description
Emplacement	Ces attributs peuvent être utilisés pour le regroupement par emplacement physique ou géographique. • Pays • State • État • Département ou province • Ville • Campus • Postal Code • Génération • Étage • Salle
Organisation	Ces attributs peuvent être utilisés pour le regroupement par organisation, mais aussi pour fournir des informations de contact. • Entreprise • Division • Business Unit • Département • Group • Contact • N° de téléphone du contact • E-mail du contact

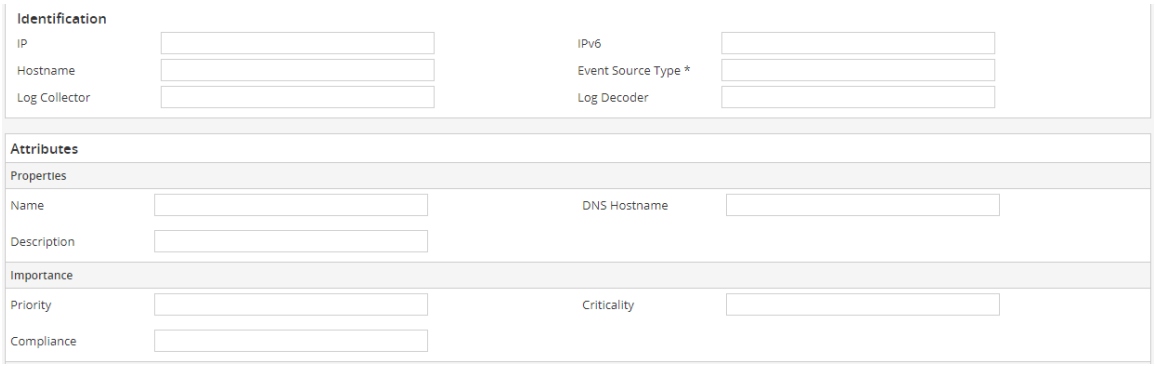
Section d'attribut	Description
Propriétaire	Ces attributs précisent les personnes responsables de la source d'événement. • Gestionnaire • Administrateur primaire • Administrateur de sauvegarde
Capacité physique	Ces attributs précisent les propriétés physiques de la source d'événement. • Vendor • Numéro de série • Balise Actif • Voltage • Protégé UPS • Hauteur du rack • Profondeur • Sortie BTU • Couleur
Fonction	Ces attributs peuvent être utilisés pour le regroupement par fonction. • Rôle principal • Sous-rôle 1 • Sous-rôle 2
System Information	Ces attributs spécifient les informations du système. • Nom du domaine • Nom du système • Identifier • Description du système

Section d'attribut	Description
Custom	Cette section fournit huit attributs personnalisés, pour tous les autres attributs dont votre organisation peut avoir besoin.

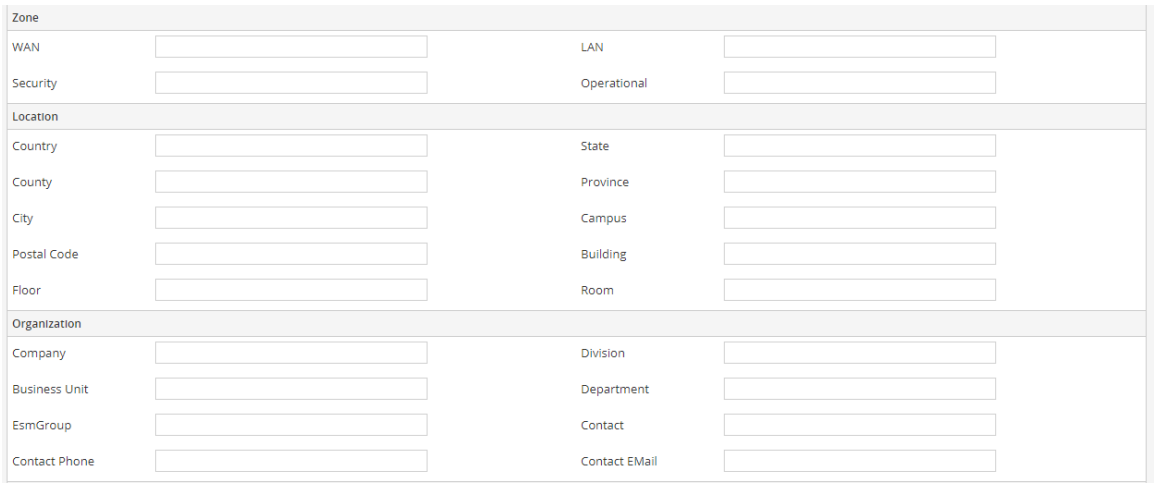
Fonctionnalités

Les paramètres de l'onglet Gérer la source d'événement sont une association d'informations remplies automatiquement et saisies par l'utilisateur. Lorsqu'une source d'événement envoie des informations de log à NetWitness Suite, elle est ajoutée à la liste de sources d'événement, et certaines informations de base sont remplies automatiquement. À tout moment par la suite, les utilisateurs peuvent ajouter ou modifier des détails pour d'autres attributs de source d'événement.

Cette figure présente un exemple des sections **Identification**, **Propriétés** et **Importance**.



Cette figure présente un exemple des sections **Zone**, **Emplacement** et **Organisation**.



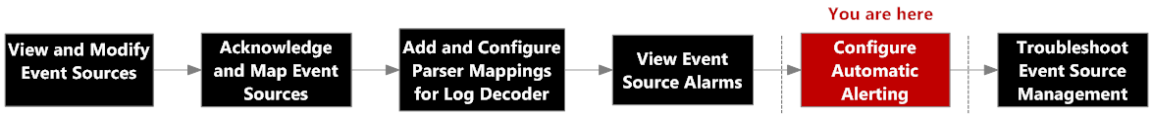
Onglet Règles de surveillance

L'onglet Règles de surveillance organise les seuils par groupe de sources d'événements.

Pour accéder à cet onglet, accédez à **ADMIN > Sources d'événements**. L'onglet **Gérer** s'affiche. Sélectionnez l'onglet **Règles de surveillance**.

Workflow

Ce workflow montre l'ensemble du processus de configuration des sources d'événements.



Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Gérer la configuration des alertes des sources d'événements.	Configuration des alertes de groupes de sources d'événements
Administrateur	Organiser des seuils par groupe de sources d'événements.	Configuration des alertes de groupes de sources d'événements

Rubriques connexes

Configuration des alertes de groupes de sources d'événements

Configuration des notifications

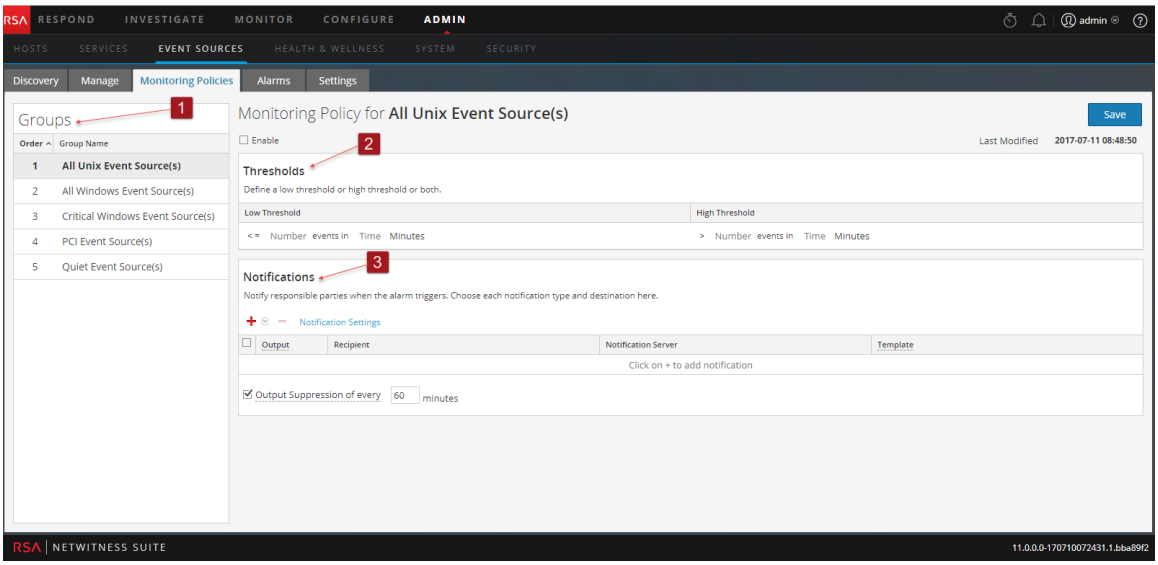
Désactivation des notifications

Aperçu rapide

La rubrique **Règles de surveillance** se compose de trois panneaux :

- Panneau Groupe d'événements
- Panneau Seuils
- Panneau Notifications

Voici un exemple de l'onglet **Règles de surveillance**.



1 Affiche le panneau Groupes.

2 Affiche le panneau Seuils.

3 Affiche le panneau Notifications.

Panneau Groupe d'événements

Le groupe sélectionné dans ce panneau détermine les seuils qui doivent être affichés dans le panneau Seuils. Vous pouvez définir un ensemble de seuils pour chaque groupe de sources d'événements. Notez que les groupes sont affiché dans un ordre spécifique :

- Faites glisser-déplacer les groupes pour modifier l'ordre spécifié.
- Les groupes placés en tête de liste sont prioritaires sur ceux qui suivent : RSA NetWitness Suite vérifie les seuils dans l'ordre prévu dans ce panneau. Ainsi, vos groupes prioritaires doivent être en haut de cette liste

Panneau Seuils

Voici un exemple du panneau Seuils pour un groupe de sources d'événements.

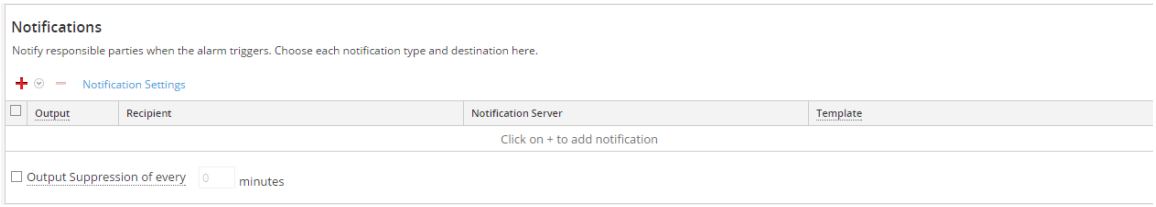
Le panneau Seuils contient les caractéristiques suivantes.

Fonctionnalité	Description
Activer	La case à cocher Activer indique si les seuils définis pour un groupe sont activés ou non. Si c'est le cas, des notifications sont envoyées chaque fois que les seuils de ce groupe dépassent la plage définie. Dans le cas contraire, aucune surveillance de ce groupe de sources d'événements n'est effectuée. **Remarque :** Si vous configurez un seuil et si vous tentez d'enregistrer la page sans l'activer, vous recevez un message de confirmation vous demandant si la règle doit être activée. Si vous activez une règle sans avoir de seuil défini, vous continuerez à recevoir des notifications automatiques (de base) tant que les notifications automatiques sont activées. Voir ci-dessous pour plus de détails sur l'apparence des notifications.
Faible nombre d'événements Faible nombre de minutes ou d'heures	Il s'agit de la limite inférieure du seuil. Saisissez le plus petit nombre d'événements et la période. Si le groupe de sources d'événements reçoit moins de messages que spécifié ici, le seuil n'est pas atteint et les notifications sont envoyées.
Nombre élevé d'événements Nombre élevé de minutes ou d'heures	Fonctionne de la même manière que pour les valeurs inférieures : Si le groupe de sources d'événements reçoit plus de messages que spécifié ici, le seuil n'est pas atteint et les notifications sont envoyées.
Date et heure de la dernière modification	Ce champ indique la date et l'heure auxquelles les seuils ont été modifiés pour la dernière fois.

Fonctionnalité	Description
Enregistrer	Enregistre les modifications que vous avez effectuées sur les seuils.

Panneau Notifications

Voici un exemple du panneau Notifications pour un groupe de sources d'événements.

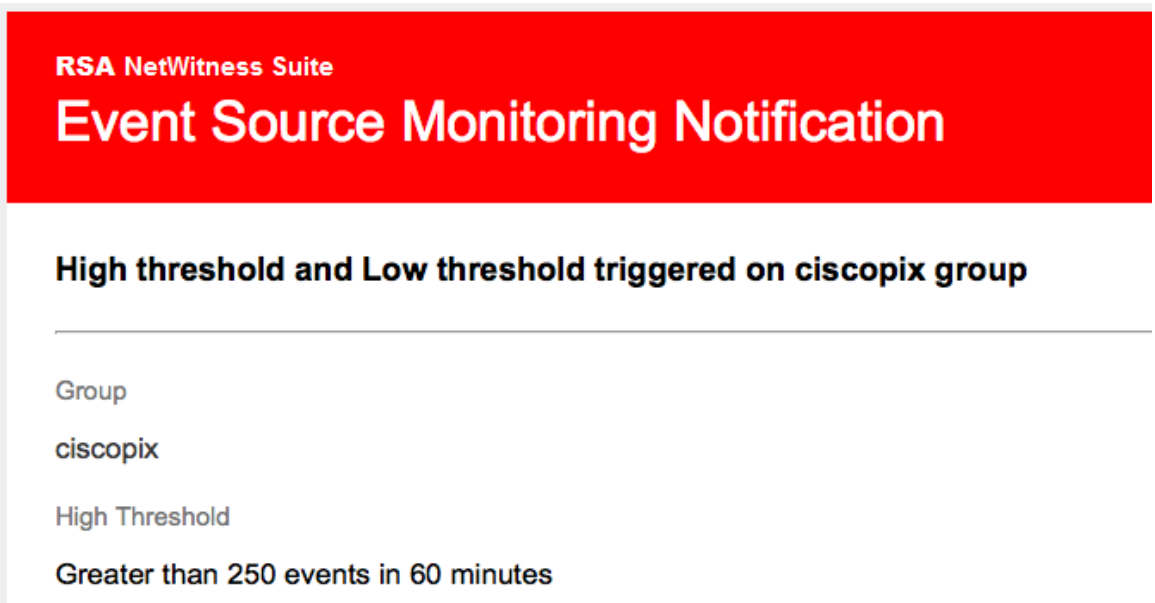


Le tableau suivant décrit les champs du panneau Notifications

Champ	Description
Outils + -	Les éléments suivants sont disponibles dans la barre d'outils : • **Ajouter (+)** : le fait de cliquer sur **Ajouter** présente un menu dans lequel vous pouvez choisir le type de notification • **Supprimer (-)** : supprime la ligne sélectionnée de la liste.
Paramètres de notification	Cliquer sur ce lien permet d'ouvrir un nouvel onglet de navigateur et de vous renvoyer à la page **Administration** > **Système** > **Notifications** dans NetWitness Suite.
Type	Affiche le type de la notification que vous avez choisie. Les options disponibles sont les suivantes : • E-mail • SNMP • Syslog
Notification	Consultez le**Configurer les sorties de Notification**rubrique dans le*Guide de Configuration système*Pour plus d'informations.
Serveur de notification	Consultez le**Configurer les serveurs de Notification**rubrique dans le*Guide de Configuration système*Pour en savoir plus

Champ	Description
Modèle	Pour la gestion de la source d'événements, RSA fournit trois modèles prêts à l'emploi pour les notifications. Vous pouvez utiliser ces modèles tels quels ou les personnaliser en fonction des besoins de votre organisation : • **Modèle d'e-mail** : envoie des notifications aux adresses e-mail spécifiées. • **Modèle SNMP** : envoie des notifications au serveur SNMP spécifié. • **Modèle Syslog** : envoie des notifications au serveur Syslog spécifié. Consultez le**Configurer le système pour les Notifications**rubrique dans le*Guide de Configuration système*Pour plus d'informations.
Limitation des sorties	Utilisez cette option pour limiter la fréquence de réception des notifications de cette règle, en cas de déclenchement d'une multitude d'alertes sur une courte période.

Voici des exemples de notifications basées sur les modèles fournis :



- E-mail :

  Pour les notifications par e-mail, la troisième colonne, **Type d'alarme**, indique si l'alarme déclenchée a été basée sur un seuil défini par l'utilisateur ou sur les données de base dépassant les limites normales. Si la surveillance ou les notifications automatiques sont désactivées, vous ne recevrez pas de notifications **automatiques**. Cela est également vrai pour Syslog et SNMP, sauf que ces notifications sont mises en forme différemment.

- Trap SNMP :

```
11-11-2015 11:57:33 Local7.Debug 127.0.0.1 community=public,
enterprise=1.3.6.1.4.1.36807.1.20.1, uptime=104313, agent_
ip=10.251.37.92, version=Ver2,
1.3.6.1.4.1.36807.1.20.1="NetWitness Suite Event Source
Monitoring Notification:
Group: PCI Event Source(s)
High Threshold:
Greater than 500 events in 5 minutes
10.17.0.10,ciscopix,Manual
10.17.0.13,ciscopix,Manual
10.17.0.8,ciscopix,Manual
10.17.0.8,ciscopix,Automatic
10.17.0.12,ciscopix,Manual
10.17.0.5,ciscopix,Manual
10.17.0.6,ciscopix,Manual
10.17.0.4,ciscopix,Manual
10.17.0.4,ciscopix,Automatic
10.17.0.3,ciscopix,Manual"
```

- Exemple Syslog :

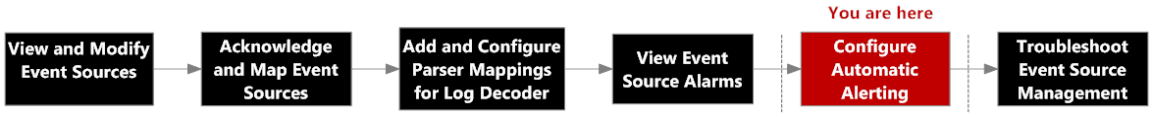
```
11-11-2015 11:57:33 User.Info 127.0.0.1 Nov 11 11:57:33
localhost CEF:0|RSA|NetWitness Suite Event Source
Monitoring|10.6.0.0.0|
HighThresholdAlert|ThresholdExceeded|1|cat=PCI Event Source
(s)|Devices|
src=10.17.0.10,ciscopix,Manual|src=10.17.0.13,ciscopix,Manual|sr
c=10.17.0.8,ciscopix,Manual|src=10.17.0.8,ciscopix,Automatic|src
=10.17.0.12,ciscopix,Manual|src=10.17.0.5,ciscopix,Manual|src=10
.17.0.6,ciscopix,Manual|src=10.17.0.4,ciscopix,Manual|src=10.17.
0.4,ciscopix,Automatic|src=10.17.0.3,ciscopix,Manual|
```

Onglet Paramètres

L'onglet Paramètres présente des options pour la surveillance automatique (alertes de base). Pour accéder à cet onglet, accédez àADMIN> Sources d'événements > Paramètres.

Workflow

Ce workflow montre l'ensemble du processus de configuration des sources d'événements.



Que voulez-vous faire ?

Rôle	Je souhaite...	Documentation
Administrateur	Configurer des règles et des seuils pour vos groupes de sources d'événements afin que vous receviez des notifications par e-mail lorsque les seuils ne sont pas atteints.	Configuration des notifications
Administrateur	Afficher ou modifier le comportement des alertes de base.	Configuration des alertes de groupes de sources d'événements

Rubriques connexes

Alertes automatiques

Configuration des notifications

Désactivation des notifications

Aperçu rapide

Vous pouvez configurer des règles et des seuils pour vos groupes de sources d'événements. Cela vous permet de recevoir des notifications lorsque les seuils ne sont pas atteints. NetWitness Suite comporte aussi un moyen automatique de recevoir des alarmes si vous ne souhaitez pas configurer des seuils au delà desquels générer des alarmes.

À propos des alertes automatiques

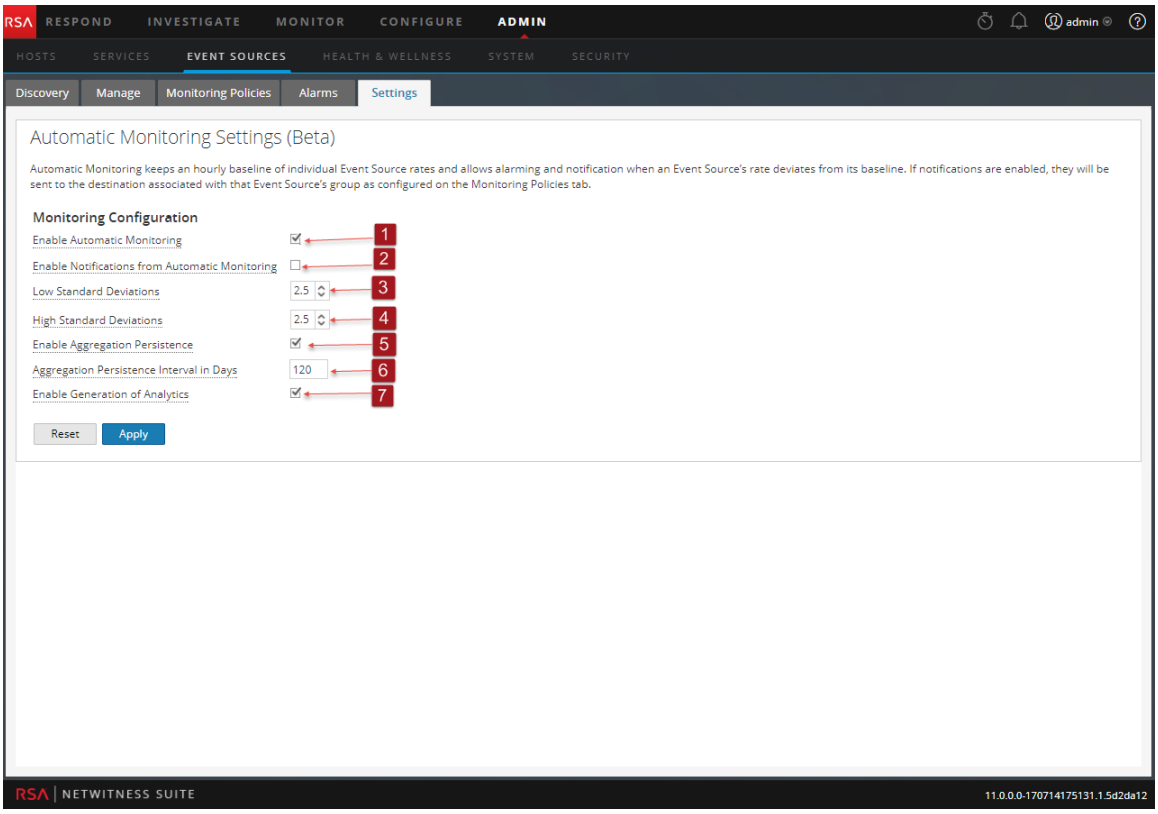
Vous pouvez définir des règles et des seuils pour vos groupes de sources d'événements afin de recevoir des notifications lorsque les seuils ne sont pas respectés. NetWitness Suite fournit aussi un moyen automatique de recevoir des alarmes si vous ne souhaitez pas configurer des seuils au delà desquels générer des alarmes.

Pour déclencher des alertes automatiques, vous pouvez utiliser les valeurs de base. Ainsi, vous n'avez pas besoin de configurer de nombreux seuils de groupe ni un tas de règles en vue de recevoir ces alertes. Une quantité anormale de messages suffit à provoquer le déclenchement des alertes, sans avoir à effectuer une configuration particulière (sauf pour activer une alerte automatique).

Notez les points suivants :

- Dès que vous commencez à collecter des messages provenant d'une source d'événement, il faut environ une semaine pour que le système puisse stocker une valeur de référence pour cette source d'événement. Après cette période initiale, le système vous avertit lorsque le nombre de messages sur une période est supérieur ou inférieur à la ligne de base pour une quantité donnée. Par défaut, cette quantité correspond à un écart-type de 2 au-dessus ou en dessous de la ligne de base.
- Basez vos paramètres d'écarts supérieur et inférieur sur la « régularité » du comportement de vos sources d'événements. Autrement dit, si vous vous attendez à peu ou pas de variation dans le nombre de messages qui arrivent pendant une période donnée (par exemple, entre 08:00 et 09:00 un jour de semaine), vous pouvez définir une valeur faible pour l'écart. Inversement, si vous constatez souvent des pics et des creux, vous pouvez définir une valeur d'écart supérieure.
- Si vous activez une règle sans avoir de seuil défini, vous continuerez à recevoir des notifications automatiques (de base) tant que l'alerte automatique est activée.

Remarque : Les alertes automatiques, et leurs paramètres, sont actuellement en phase de test bêta.



1	Détermine si les alertes automatiques sont activées ou désactivées. Par défaut, cette option est sélectionnée (alertes automatiques activées)
2	Détermine si les notifications des alertes automatiques sont activées ou désactivées. Par défaut, cette option est désactivée (les notifications automatiques ne sont pas envoyées lorsque les alertes automatiques se déclenchent)
3	Seuil d'écarts types en dessous duquel les alertes doivent être reçues. La valeur par défaut est **2,0** (95 % de confiance)
4	Seuil d'écarts types au-dessus duquel les alertes doivent être reçues. La valeur par défaut est **2,0** (95 % de confiance)
5	Une fois sélectionnée, cette option stocke le nombre de sources d'événements par intervalle d'une heure. Les données collectées sont utilisées pour former les valeurs de référence de chaque source de l'événement. • **Activé (par défaut)** : un nombre par heure et par source de l'événement est stocké dans la base de données sous-jacente. Ces nombres par heure (ou agrégations) constituent la base historique du calcul de la plage normale pour chaque source de l'événement. • **Désactivé** : lorsque le serveur SMS redémarre, la surveillance des sources d'événements ne comporte aucune donnée historique permettant de calculer la plage

	normale. L'utilisateur doit attendre que suffisamment de données (l'équivalent d'une semaine environ) soient collectées pour former une nouvelle base pour chaque source de l'événement
6	Contrôle la quantité de données historiques (reportez-vous à **Activer la persistance de l'agrégation**) à conserver pour chaque source de l'événement. La valeur par défaut est de 120 jours, ce qui signifie que 4 mois d'historique environ sont conservés, puis utilisés lors de la reconstruction de la base pour chaque source de l'événement.
7	Une fois cette option activée, les données relatives au comportement des alertes automatiques sont stockées sur disque. La valeur par défaut est **Activé**. Les données conservées comprennent la valeur de base au fil du temps et l'historique des alertes pour chaque source de l'événement. Toutefois, notez que l'adresse et le type de la source de l'événement sont anonymes. Par conséquent, seules les informations relatives au taux d'événements sont révélées. Dans la mesure où les alertes automatiques sont une fonction bêta, ces données sont importantes pour mesurer l'efficacité de la fonction. Vous pouvez désactiver cette option. Cela n'affecte pas la fonction d'alerte automatique.
8	L'option **Réinitialiser** indique que les modifications sont ignorées pour tous les paramètres de la page.
9	Cliquez sur **Appliquer** pour enregistrer les modifications apportées aux valeurs de la page.

Fonctions

L'onglet Paramètres contient les fonctions suivantes.

Fonctionnalité	Description
Activer la surveillance automatique	Détermine si les alertes automatiques sont activées ou désactivées. Par défaut, cette option est sélectionnée (alertes automatiques activées)
Activer les notifications en mode Surveillance automatique	Détermine si les notifications des alertes automatiques sont activées ou désactivées. Par défaut, cette option est désactivée (les notifications automatiques ne sont pas envoyées lorsque les alertes automatiques se déclenchent)

Fonctionnalité	Description
Écarts types faibles	Seuil d'écarts types en dessous duquel les alertes doivent être reçues. La valeur par défaut est **2,0** (95 % de confiance)
Écarts types élevés	Seuil d'écarts types audessus duquel les alertes doivent être reçues. La valeur par défaut est **2,0** (95 % de confiance)
Activer la persistance de l'agrégation	Une fois sélectionnée, cette option stocke le nombre de sources d'événements par intervalle d'une heure. Les données collectées sont utilisées pour former les valeurs de référence de chaque source de l'événement. • Activé (par défaut) : un nombre par heure et par source de l'événement est stocké dans la base de données sous-jacente. Ces nombres par heure (ou agrégations) constituent la base historique du calcul de la plage normale pour chaque source de l'événement. • Désactivé : lorsque le serveur SMS redémarre, la surveillance des sources d'événements ne comporte aucune donnée historique permettant de calculer la plage normale. L'utilisateur doit attendre que suffisamment de données (l'équivalent d'une semaine environ) soient collectées pour former une nouvelle base pour chaque source de l'événement
Intervalle de persistance de l'agrégation en jours	Contrôle la quantité de données historiques (reportez-vous à **Activer la persistance de l'agrégation**) à conserver pour chaque source de l'événement. La valeur par défaut est de 120 jours, ce qui signifie que 4 mois d'historique environ sont conservés, puis utilisés lors de la reconstruction de la base pour chaque source de l'événement.

Fonctionnalité	Description
Activer la génération d'analyses	Une fois cette option activée, les données relatives au comportement des alertes automatiques sont stockées sur disque. La valeur par défaut est **Activé**. Les données conservées comprennent la valeur de base au fil du temps et l'historique des alertes pour chaque source de l'événement. Toutefois, notez que l'adresse et le type de la source de l'événement sont anonymes. Par conséquent, seules les informations relatives au taux d'événements sont révélées. Dans la mesure où les alertes automatiques sont une fonction bêta, ces données sont importantes pour mesurer l'efficacité de la fonction. Vous pouvez désactiver cette option. Cela n'affecte pas la fonction d'alerte automatique.
Réinitialiser	Cette option indique que les modifications sont ignorées pour tous les paramètres de la page.
Appliquer	Cliquez sur **Appliquer** pour enregistrer les modifications apportées aux valeurs de la page.